

2018

# Defense in Depth Network Perimeter Security

Anuoluwapo Ope Fatokun

*Eastern Illinois University*

This research is a product of the graduate program in [Technology](#) at Eastern Illinois University. [Find out more](#) about the program.

---

## Recommended Citation

Fatokun, Anuoluwapo Ope, "Defense in Depth Network Perimeter Security" (2018). *Masters Theses*. 3560.  
<https://thekeep.eiu.edu/theses/3560>

This is brought to you for free and open access by the Student Theses & Publications at The Keep. It has been accepted for inclusion in Masters Theses by an authorized administrator of The Keep. For more information, please contact [tabruns@eiu.edu](mailto:tabruns@eiu.edu).



## Thesis Maintenance and Reproduction Certificate

FOR: Graduate Candidates Completing Theses in Partial Fulfillment of the Degree  
Graduate Faculty Advisors Directing the Theses

RE: Preservation, Reproduction, and Distribution of Thesis Research

Preserving, reproducing, and distributing thesis research is an important part of Booth Library's responsibility to provide access to scholarship. In order to further this goal, Booth Library makes all graduate theses completed as part of a degree program at Eastern Illinois University available for personal study, research, and other not-for-profit educational purposes. Under 17 U.S.C. § 108, the library may reproduce and distribute a copy without infringing on copyright; however, professional courtesy dictates that permission be requested from the author before doing so.

Your signatures affirm the following:

- The graduate candidate is the author of this thesis.
- The graduate candidate retains the copyright and intellectual property rights associated with the original research, creative activity, and intellectual or artistic content of the thesis.
- The graduate candidate certifies her/his compliance with federal copyright law (Title 17 of the U. S. Code) and her/his right to authorize reproduction and distribution of all copyrighted materials included in this thesis.
- The graduate candidate in consultation with the faculty advisor grants Booth Library the nonexclusive, perpetual right to make copies of the thesis freely and publicly available without restriction, by means of any current or successive technology, including but not limited to photocopying, microfilm, digitization, or internet.
- The graduate candidate acknowledges that by depositing her/his thesis with Booth Library, her/his work is available for viewing by the public and may be borrowed through the library's circulation and interlibrary loan departments, or accessed electronically. The graduate candidate acknowledges this policy by indicating in the following manner:

☒ Yes, I wish to make accessible this thesis for viewing by the public

☐ No, I wish to quarantine the thesis temporarily and have included the **Thesis Withholding Request Form**

- The graduate candidate waives the confidentiality provisions of the Family Educational Rights and Privacy Act (FERPA) (20 U. S. C. § 1232g; 34 CFR Part 99) with respect to the contents of the thesis and with respect to information concerning authorship of the thesis, including name and status as a student at Eastern Illinois University. I have conferred with my graduate faculty advisor. My signature below indicates that I have read and agree with the above statements, and hereby give my permission to allow Booth Library to reproduce and  
signature indicates concurrence !

Graduate Candidate Signature

Anuoluwapo Ope Fatokun

Printed Name

M.Sc. Technology

Graduate Degree Program

Faculty Adviser Signature

David W. Melton

Printed Name

8 May 2018

Date

Please submit in duplicate.

---

DEFENSE IN DEPTH  
NETWORK PERIMETER  
SECURITY

---

BY

---

Anuoluwapo Ope Fatokun

---

THESIS

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE DEGREE OF

---

Master of Science in Technology

---

IN THE GRADUATE SCHOOL, EASTERN ILLINOIS UNIVERSITY  
CHARLESTON, ILLINOIS

---

2018  
YEAR

---

I HEREBY RECOMMEND THAT THIS THESIS BE ACCEPTED AS FULFILLING  
THIS PART OF THE GRADUATE DEGREE CITED ABOVE

5/1/18

DATE

5/9/18

DATE

THESIS COMMITTEE MEMBER

5/1/18

DATE

---

THESIS COMMITTEE MEMBER

DATE

THESIS COMMITTEE MEMBER

5/5/18

DATE

---

THESIS COMMITTEE MEMBER

DATE

**Copyright © 2018 by Anuoluwapo Ope Fatokun**

**All Rights Reserved**

## ABSTRACT

Defense in depth network perimeter security has always be a topic of discussion for a long time as an efficient way of mitigating cyber-attacks. While there are no 100% mitigating method against cyber-attacks, a layered defense in depth network perimeter security can be used to mitigate against cyber-attacks. Research have shown a massive growth in cyber-crimes and there are limited number of cyber security expert to counter this attacks. EIU as an institution is taking up the responsibility of producing cyber security graduates with the new Master of Science in Cyber Security program that started in Fall 2017.

This research is aim at designing and developing a defense in depth network perimeter security that will be used for laboratory practices to learn and simulate cyber security activity and its mitigation. The research is complemented with the design of ten laboratory practices to give expertise to the students in the equipment used in the design. The designed topology comprises of two sites, connected via IPSec site to site VPN over an unsecure internet connection. A public testing webserver is placed at the DMZ which is to be used to invite hackers to attack the design system for the purpose of detecting, preventing and learning cyber-attack mechanisms.

## DEDICATION

I dedicate this thesis to God Almighty for His love towards me and in loving memory of my late parents; Mr & Mrs Caleb Fatokun. Their labor over me was never in vain.

## ACKNOWLEDGMENT

First, I sincerely thank and appreciate my supervisor Dr. Rigoberto Chinchilla, for his supervision, input, guidance and mentorship during the course of this thesis and my graduate program at EIU. I specially want to appreciate the trust and confidence he repose in me for giving me the opportunity to serve under him as his graduate research assistant in the Cyber Security program.

I am also grateful to members of my thesis committee; Dr. Israr Toqeer and Dr. Wutthigrai Boonsuk for accepting to serve on my committee and for providing valuable suggestions for my thesis. I also want to thank the coordinator of my program Dr. David Melton who constantly ask about the progress of my thesis and always ready to listen to me anytime I have an issue. I also appreciate Dr. Jerry Cloward for his smiles and questions regarding the progress of my thesis. Also special thanks to Dr. Odai Y. Khasawneh & Dr. Rendong Bai both who my office share demarcation with and sometimes disturb them with calls.

My gratitude also go to the Information Technology Services (ITS) team who came to my aid when I couldn't get access to the server I used in my research and for always coming to fix issues when I ran into any.

Special appreciation to my wife Oluwafunmilola Olawanle Fatokun for her support, love and understanding. Thank you for allowing me to always spend those nights reading and studying. You have been the pillar of my success stories. God bless and keep you for me.

Lastly, I want to appreciate my siblings Dre, Yomi, Sis AY, Joke and the Twins for the supports, love and prayers. May God continue to bind the bond between us.

I will not fail to appreciate a brother from another mother, Adekunle Adeyemo, you have been a brother since the days of undergraduate, and you are the reason why I came for my master degree program, thank you for always standing by me and for your mentorship. And to all the friends I made during the course of the program and most especially to my graduate assistant colleague Mohammad Mohsen, you are a kind and very loving guy. You always there to watch my back. Thank you so much! Ebede, Kenny, Dayo thank you all for making my graduate program a memorable one.



## TABLE OF CONTENTS

ABSTRACT.....	iii
DEDICATION.....	iv
ACKNOWLEDGMENT.....	v
INTRODUCTION.....	1
Justification of the Study.....	2
Overall Aim.....	3
Objectives.....	3
Hypothesis.....	4
Delimitations.....	5
REVIEW OF LITERATURE.....	6
Cyber Security and its Challenges.....	6
Notable Cyber Attacks.....	7
Cyber Attacks Mitigating Techniques.....	8
Virtual Private Network (VPN) Techniques.....	9
Firewall Technology.....	9
Intrusion Detection Systems.....	10
Intrusion Prevention Systems.....	14
METHODOLOGY.....	20
The Design Topology.....	20
The Router.....	21
The Palo Alto Firewall/IDS.....	24
Webserver Configuration.....	32
Cisco ASA Firewall Configuration and the Internal Router.....	33
The EIU Satellite Campus Gateway Router and the Firewall/IDS.....	33
Virtual Private Network.....	35
RESULTS.....	36
Results and Discussion.....	36
Conclusion.....	42
Recommendation.....	43
REFERENCES.....	44
APPENDICES.....	49
Appendix A – Definition of Terms.....	50
Appendix B – Configuration of EIU Main Gateway Router.....	51
Appendix C – Configuration of Cisco ASA Firewall.....	54
Appendix D – Configuration of Internal Router.....	57
Appendix E – Configuration of EIU Satellite Campus Gateway Router.....	59
Appendix F – Laboratory Guidelines.....	62

## LIST OF FIGURES

Figure 2. 1 VPN site to site and from roaming users.....	9
Figure 2. 2 Firewall location in a network.....	10
Figure 2. 3 The DMZ.....	10
Figure 2. 4 Host Based IDS.....	13
Figure 2. 5 A NIDS.....	14
Figure 2. 6 A HIPS.....	17
Figure 2. 7 A NIPS.....	18
Figure 3. 1 The Topology for the Defense in Depth Network Perimeter Security for the EIU Cyber Security Lab.....	21
Figure 3. 2 Port forwarding configuration on the Verizon hotspot.....	23
Figure 3. 3 Creating a Zone.....	25
Figure 3. 4 Interface configuration.....	26
Figure 3. 5 IP address configuration on the interface.....	26
Figure 3. 6 Virtual Routers.....	27
Figure 3. 7 Virtual Router Configuration.....	28
Figure 3. 8 Static Route configuration.....	29
Figure 3. 9 Attaching an interface to a Virtual Router.....	30
Figure 3. 10 Security Policies.....	31
Figure 3. 11 DoS Protection configuration.....	32
Figure 3. 12 EIU Satellite Campus Champaign.....	34
Figure 4. 1 EIU Main Campus Internal LAN User (10.234.100.50/24) ping www.google.com.....	37
Figure 4. 2 EIU Satellite Campus Champaign Internal LAN User (10.234.200.50/24) ping www.google.com.....	38
Figure 4. 3 EIU Main Campus Internal User accessing the Webserver through Private IP address 172.16.1.2.....	39
Figure 4. 4 Internet User access the webserver through the public IP address 166.165.203.151.....	40
Figure 4. 5 EIU Main Campus Internal LAN User (10.234.100.50) pinging EIU Satellite Campus.....	41
Figure 4. 6 EIU Satellite Campus Internal LAN User (10.234.200.50) pinging EIU Main Campus.....	42

## CHAPTER I

### INTRODUCTION

In the light of all the headline-grabbing network and cyber security breaches in the last few years ranging from Equifax hacking to the alleged USA presidential election hacking and the recently announced Yahoo hacking among others. It's understandable that enterprises might be on high alert to prevent their own organization from being thrust into the spotlight, unfortunately there are no best solution to this because today's cyber criminals are just too persistent [1]. A multiple layered defense in depth strategy for network perimeter security can provide an answer to mitigate cyber security attacks. Putting a number on the cost of cybercrime and cyber espionage is the headline, but the dollar figure may not take in account the damage to the victims due to the cumulative effect of losses in cyberspace [2].

We operate in a real world of system misconfigurations, software bugs, disgruntled employees, and overloaded system administrators [3]. The increasing sophisticated nature of cyber-attacks on computer networks these days has rendered most of the traditional firewalls inefficient; even the most complex ones are insufficient for protecting attacks from general computer networks [4]. The defense in depth's strategy of network perimeter security helps in protecting network resources even if one of the security layer is compromised [3].

In the past, IT executives have concentrated their efforts in perimeter hardening by carefully firewalling all points of entry on their network connected to the third parties with hope that if you locked down access to your network, you would automatically protect applications, data and resources [5]. Outsiders are not always the only bad guys, insiders commit the majority of computer security breaches. According to CSI/FBI 2003 survey, nearly 80% of computer security breaches are done by insiders [6]. Defense in depth network

perimeter security allows to protect your network with multiple layers of security such that if one layer of security is compromised or hackers was able to get through it, another layers of security is there to further protect the network. In this research, we make use of different security vendor (Cisco & Palo Alto) to achieve our multiple layer defense in depth network perimeter security. One of the advantages of using different vendors is to provide an additional level of security such that an attack that could pass through a security vendor devices because of a known bug might not be available to pass through the other security vendor devices and thereby providing more security for the network.

#### Justification of the Study

The complexities of cyber-attacks are increasing every day, hackers are working around the clock developing hacking tools and new way of how to break into the assumed most secured network. Events in the last few months have proved that even the most secured network are still prone to cyber-attacks, recent examples include the Equifax hack [7], the alleged Russian Cyber hack on U.S Electoral system [8], the Yahoo account hack [9]. In fact, Kevin G. Coleman [10] reported a statement credited to Casteel; a manager at SCADA that “We would never be able to completely get ahead of cyber criminals perpetuating cyber-attacks”. Casteel statement is a call for more research and awareness in the area of cyber security, improve security techniques and strategies in order to combat security attacks. Yet, there are not enough skilled people to combat this increasing cyber-attack menace, in fact, according to Tripwire study [11], 75 percent of organizations lack skilled cyber security experts.

Academic institutions, especially universities, are beginning to realize the urgent need for more research and programs in cyber security to develop and design cyber security

techniques and strategies to combat cyber security attacks and thereby producing cyber security graduates with the necessary skills to meet up the increasing challenge of cyber-attacks. Eastern Illinois University started a Cyber Security Master's program under the School of Technology to meet its responsibility of producing graduates capable of fulfilling the world challenges in this area. This study will contribute to the Cyber Security Ms. Program by developing a defense in depth network perimeter security design for practical learning among different courses within the program. Providing laboratory training would further reinforce and expose students to different technologies used in most organizations [12]. This study will implement a typical enterprise branch-headquarters defense in depth network perimeter security and would help the students to gain practical experience on a typical network scenario that they might come across after their graduation.

#### Overall Aim

This thesis will propose a defense in depth network perimeter security design for the new Master of Science Cyber Security at Eastern Illinois University. This study is advancing on previous design and works by incorporating cyber security technology such as IPSec Site to Site Virtual Private Network (VPN), Remote Access VPN, and Network Security Device High Availability. This thesis will provide the student with a real life practical experience and exposure they might come across after the completion of their program.

#### Objectives

1. Design a defense in depth network perimeter security architecture with a VPN solution to a simulated branch site for the MSc Cyber Security Laboratory at EIU.



2. Develop a perimeter security architecture as a practice network scenario to learn cyber security technologies such as IPSec Site-to-Site VPN, Remote Access VPN, Network Security Device High Availability, and Network device hardening.
3. Design and develop at least ten different laboratory guides comprising of how to use the designed perimeter network. Some of the laboratory guides includes packet filtering, NAT, HTTP Inspection etc. using cisco ASA and Palo Alto firewalls.
4. Simulate using the developed architecture cyber security attacks.
5. Recommend a detailed future work and development of the laboratory.

### Hypothesis

The intent of this research is to ascertain the following:

It is possible to:

1. Develop a defense in depth network perimeter security that would offer a high resiliency to cyber-attacks within academic setting of the EIU Cyber Security Laboratory.
2. Develop a defense in depth network perimeter security that would offer high availability for the network security devices and thereby continuously protecting against cyber-attacks in event of failure of one of the security device.
3. Develop and test a defense in depth network perimeter security that would offer multi-vendor layered security and thereby providing security against cyber-attacks in event hackers breaks through a security vendor device.
4. Develop, test and simulate an IPSec site-to-site VPN that offers secure communication over unsecured internet network.

5. Provide students with cyber-attacks real experience, and to teach them how to further improve cyber security systems based on the EIU laboratory experience.

#### Delimitations

This research would strictly provide a design for a defense in depth network perimeter security for the purpose of testing how a multilayer defense could protect against network attacks, and would not discuss the speed or the full implementation of the designed system. Also the Palo Alto used in the design (PA 200) is limited to HA lite; that is, it cannot do a stateful high availability. In addition, just basic security such as port security would be configured on the switch, and no extensive switch security would be considered.

There is also the possibility that hackers launch sophisticated attackers that can break the security of designed system due to the fact that we do not have the latest IOS security versions and updated equipment.

There is also possibility that no hackers will launch an attack to the designed system, although past experiences have demonstrated that hackers have very quickly found and attack our network.

## CHAPTER II

### REVIEW OF LITERATURE

#### Cyber Security and its Challenges

Cyber security is the practice of protecting systems, networks, and programs from attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes. Implementing effective cyber security measures is particularly challenging today because there are more devices than people, and attackers are becoming more innovative [15].

The twenty first century has seen a new dimension of warfare; the cyber warfare. Developed countries have started exploiting the vulnerabilities of cyberspace to gain supremacy and influence over the rivals and over countries. Projects like PRISM and Boundless Information and malwares like Stuxnet and Distrack have surprised the world by revealing how the cyberspace is being exploited by developed countries [14]. Reliance of developing countries on a reliable and secure cyberspace do not match with that of western world but still few of their critical organizations like national, military and private sector hold significant share in cyberspace. Mostly, these developing countries rely on the products developed by western world. The dependency has inherent vulnerabilities and opportunities which place their critical organizations vulnerable to cyber exploitation [14].

The Internet of Things (IoT) has been the major subject in the IT world, with the reality of IoT there would be more complexity as more devices than ever are expected to be interconnected. According to Folk et al [13], over a billion devices are expected to be interconnected, and with this comes unimaginable exploits, vulnerabilities, and attacks.



A successful cyber security approach has multiple layers of protection spread across the computers, networks, program, or data that one intends to keep safe. In an organization, the people, processes, and technology must all complement one another to create an effective defense from cyber-attacks [13].

### Notable Cyber Attacks

Bombshell hacks were revealed one after another in 2017, from an Equifax breach that compromised almost half the country to global ransom campaigns that cost companies millions of dollars. The cyber-attacks highlighted the alarming vulnerability of our personal information.

More tools used by government hackers have become public, and it's easier than ever to create sophisticated ways to spread malware or ransomware or steal data from companies. Companies also frequently fail to patch security flaws in a timely manner [16]. Mark Nunnikhoven said as we do more and more of our business online, and as criminals realize the value of the data that organizations are protecting, we're seeing more big-name breaches, more high-profile breaches [17].

In particular, ransomware when hackers demand money to unlock files is becoming more common. In 2017, Bitdefender, an antivirus software firm found out that ransomware payments hit \$2 billion twice as much as in 2016 and it was predicted by trend micro that it will exceed \$9 billion the following year [18].

Cybercriminals penetrated Equifax, one of the largest credit bureaus, in July and stole the personal data of 145 million people [16]. It was considered among the worst breaches of all time because of the amount of sensitive information exposed, including Social Security numbers. The company only revealed the hack two months later. This attack could have an impact for years because the stolen data could be used for identity theft.

The Equifax breach raised concerns over the amount of information data brokers collect on consumers, which can range from public records to mailing addresses, birth dates and other personal details. Firms like Equifax, TransUnion and Experian sell that data to customers, such as banks, landlords and employers, so they can learn more about each and every one. Whether data brokers do enough to keep that private information secure is under scrutiny [16].

Cellebrite is a company that produces devices that can pull personal data from mobile phones to be use by the military and the government. The company fell victim to their own game when their external web server was hacked and 900GB of customer information and technical product data was taken [19].

NHS – Though not targeted specifically at the NHS, the WannaCry Ransomware most notably struck the UK health service, preventing workers from accessing their computers and delaying vital medical procedures. Fortunately, a flaw in its mechanism allowed experts to create a kill switch [19].

In June, a security researcher discovered almost 200 million voter records exposed online after a GOP data firm misconfigured a security setting in its Amazon cloud storage service. It was the latest in a string of major breaches stemming from insecure Amazon servers where data is stored. They are secure by default, but Chris Vickery, a researcher at cybersecurity firm UpGuard, regularly finds that companies set it up wrong [20].

### Cyber Attacks Mitigating Techniques

There are several techniques or technology that are always been deployed by the government, cooperate bodies and individuals in order to mitigate cyber-attacks and keep their network and resources safe. Some of these technologies are discussed below.

### Virtual Private Network (VPN) Techniques

A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely [21]. VPN technology is widely used in corporate environments where regional offices are connected over unsecure connection such as internet as shown in Figure 2.1 [21][22].

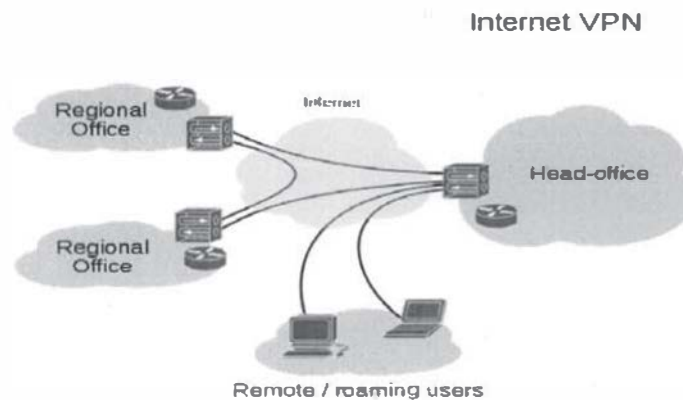


Figure 2. 1 VPN site to site and from roaming users.

### Firewall Technology

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules [22]. A firewall typically establishes a barrier between a trusted internal network and untrusted external network, such as the Internet [23]. Cheswick and Bellovin [24] define a firewall as a collection of components or a system that is placed between two networks as shown in Figure 2.2 and Figure 2.3, and possesses the following properties:

- All traffic from inside to outside, and vice-versa, must pass through it.

- Only authorized traffic, as defined by the local security policy, is allowed to pass through it.
- The firewall itself is immune to penetration.

Traditional network firewalls prevent unauthorized access and attacks by protecting the points of entry into the network.

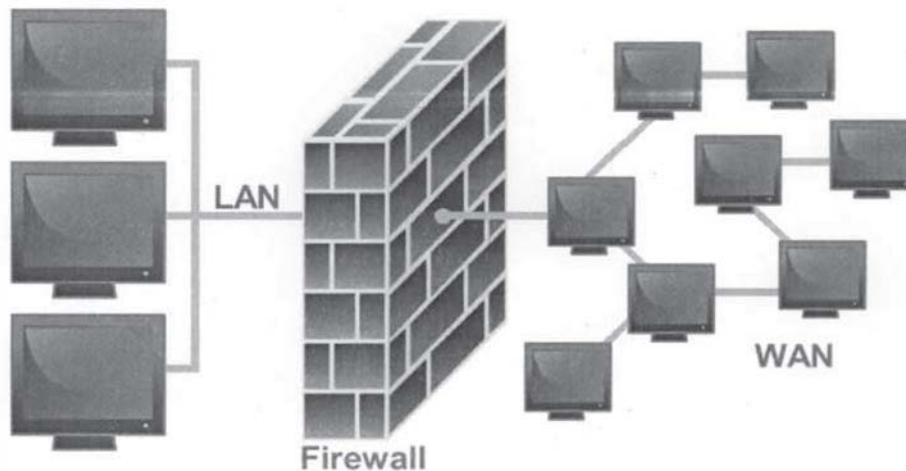


Figure 2. 2 Firewall location in a network.

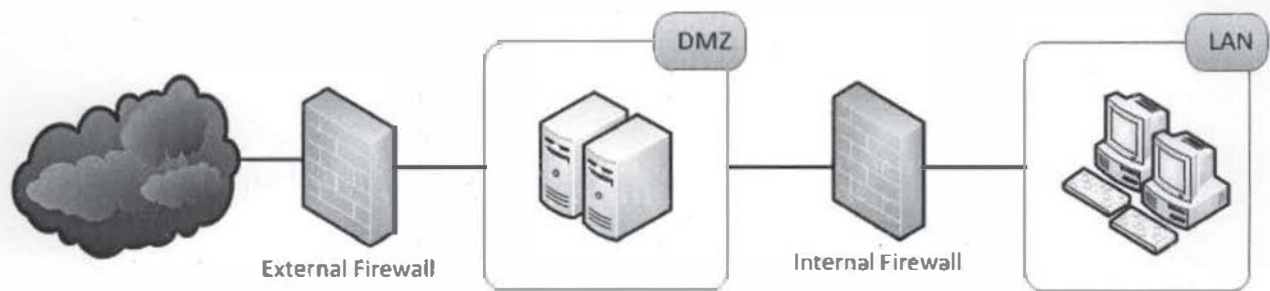


Figure 2. 3 The DMZ.

### Intrusion Detection Systems

Intrusion Detection System (IDS) defined as a device or software application which monitors the network or system activities and finds if there is any malicious activity occur. Outstanding growth and usage of internet raises concerns about how to communicate and protect the digital information safely. In today's world hackers use different types of attacks for

getting the valuable information. Many of the intrusion detection techniques, methods and algorithms help to detect those several attacks [25].

An IDS is referred as burglar alarm. For example the lock system in the house protects the house from theft. But if somebody breaks the lock system and tries to enter into the house, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm. [26]. Anderson [27] introduced the concept of intrusion detection in 1980. He has been the first showing the importance of security audit trails in the aim of detecting policy violation. He defined a violation of policy security as a deliberate unauthorized attempt to: - access information - manipulate information - make a system unreliable or unusable. Debar et al [28] also described an intrusion-detection system as a detector that processes information coming from system that is to be protected. This detector uses three kinds of information:

- Technique used to detect intrusion (for example signature database),
- Configuration information about the current state of system,
- Audit trail.

The detector eliminates all unnecessary information, determines if this action can be considered as a symptom of an intrusion, and takes an action (send alerts for example). Several types of IDS technologies exist due to the variance of network configurations. Each type has advantages and disadvantage in detection, configuration, and cost. Mainly, there are three important distinct families of IDS: The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed [29].

The first family of IDSs is Host based IDS which monitors signs of intrusion in the local system. For analysis they use host system's logging and other information, the host based handler is referred to as the sensor. Other sources, from which a host-based sensor can obtain

data, include system logs and other logs generated by operating system processes and contents of objects not reflected in standard operating system audit and logging mechanisms [30]. Host based system trust strongly on audit trail. The information of the logs allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction [31]. As shown in Figure 2.4, the elementary principle in IDS including Network Based Intrusion Detection System (NIDS) originated from anomaly HIDS research based on Denning's pioneering work [32]. A host-based IDS provides much more relevant information than Network-based IDS. HIDS are used efficiently for analyzing the network attacks, for example, it can sometimes tell exactly what the attacker did, which commands he used, what files he opened, rather than just a vague accusation and there is an attempt to execute a dangerous command [33]. It is less risky to configure.

#### Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Typically, does not require additional hardware
- Lower entry cost.



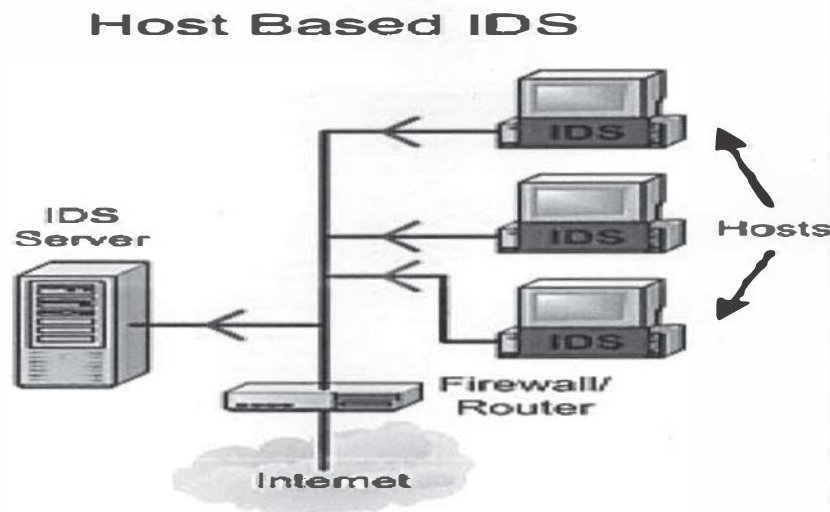


Figure 2. 4 Host Based IDS.

The second family of IDSs is the Network based IDS systems, they collect information from the network itself rather than from each separate host. The NIDS audits the network attacks while packets moving across the network. As shown in Figure 2.5, the network sensors come equipped with attack signatures that are rules on what will constitute an attack and most network-based systems allow advanced users to define their own signatures [34]. Attack on the sensor is based on signature and they are from the previous attacks and the operation of the monitors will be transparent to the users and this is also significant [35]. The transparency of the monitors decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without the efforts [31]. Network Node IDS (NNIDS) agents are deployed on every host within the network being protected [34].

#### Advantages of Network based Intrusion Detection Systems:

- Lower cost of ownership
- It is easier to deploy
- It detect network based attacks
- It retain evidence

- It provides real time detection and quick response

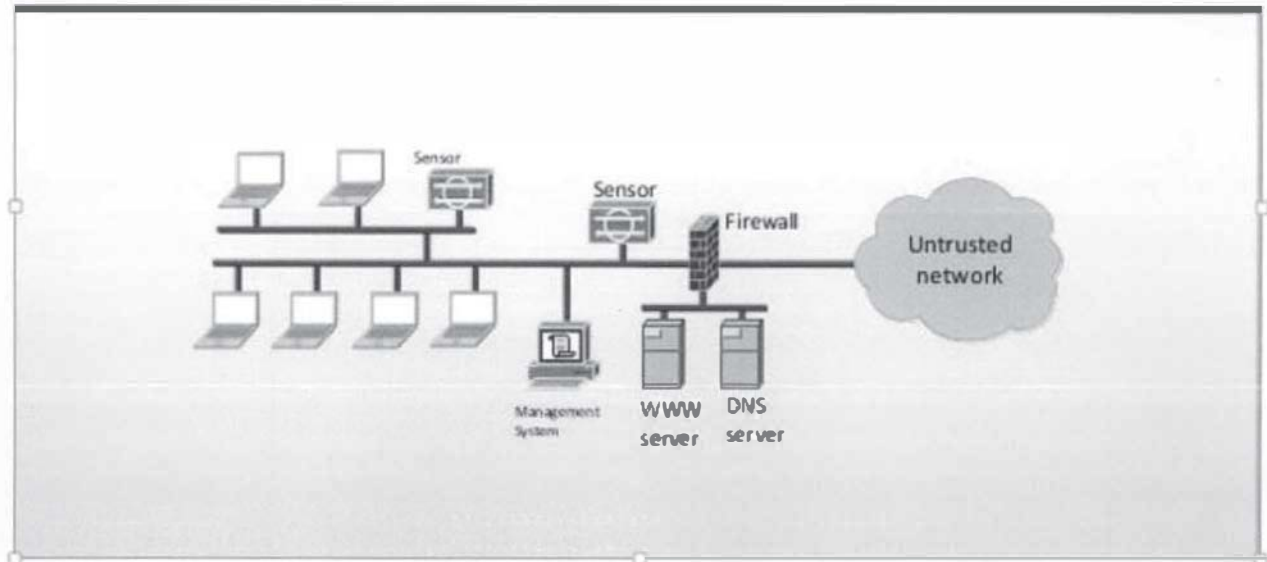


Figure 2. 5 A NIDS.

The third family of IDSs is the Application based IDS (APIDS), they check the effective behavior and event of the protocol. The system or agent is placed between a process and group of servers that monitors and analyzes the application protocol between devices [34]. Intentional attacks are the malignant attacks carried out by disgruntled employees to cause harm to the organization and unintentional attack causes financial damage to the organization for example by deleting the important data files [34].

### Intrusion Prevention Systems

Many enterprise network systems and end user devices remain susceptible to a myriad of known attacks due to a simple failure to patch known vulnerabilities, outdated equipment and malware signatures, or failure to properly setup and deploy security devices. Since known vulnerabilities are typically well documented, anyone can download ready-made tools to attack unpatched systems [36].



Newer blended threats and Advanced Persistent Threats, or APTs, use multiple old and new attack methods simultaneously, targeting specific data and even individuals within organizations. Therefore, both traditional and advanced security measures working together are especially important when defending networks against these new types of multifaceted and persistent attacks. Surveys verify the effectiveness of these new attacks, showing that in 2010, the average cost of a data breach reached \$214 per compromised record, and averaged \$7.2 million per data breach event, an increase of 6% over 2009 [37]. When developing a security strategy, organizations must plan to protect against not just current threats, but all threats, known and unknown.

Intrusion prevention system (IPSs) are an amalgam of security technologies, their goal is to anticipate and to stop attacks [38]. Instead of analyzing the traffic logs, as an IDS which lies in discovering the attacks after they took place, an Intrusion Prevention System tries to warn and prevent against such attacks. While the systems of intrusion detection try to give the alert, the Intrusion Prevention Systems block the traffic rated dangerous. Over many years, the philosophy of the intrusions detection on the network amounted to detect as many as possible of attacks and possible intrusions and to consign them so that others take the necessary measures. On the contrary, the systems of prevention of the intrusions on the network have been developed in a new philosophy "taking the necessary measures to counter attacks or detectable intrusions with precision "[38]. In general terms, IPS are always online on the network to supervise the traffic and intervene actively by limiting or deleting the traffic judged hostile by interrupting the suspected sessions or by taking other reaction measures to an attack or an intrusion. An IPS functions symmetrically to the IDS; in addition to that, they analyze connection contexts, automatize the logs analysis and suspend the suspected connections.

The need to protect data and networks, and the need to stop attacks and prevent it is the reason that the IPS was created [39]. A Firewall act like IPS, but an IPS focus on attack prevention at layers that most firewalls are not able to decipher, at least not yet [40]. There are many types of IPS like inline network intrusion detection system, application-based firewalls/IDS, layer seven switches, network-based application IDSs, and deceptive applications. An IPS is typically designed to operate completely invisibly on a network. IPS products do not typically claim an IP address on the protected network but may respond directly to any traffic in a variety of ways. As mentioned before, IPS products have ability to implement firewall rules, but it is not a core function of IPS. Also, IPS offer deeper watching and monitoring capabilities into network operations like bad logons, inappropriate content and many other network and application layer functions [41]. An IPS prevents a large amount of downtime that would occur if it were not there, this is done by stopping any damage that may have made its way to the databases from internal or even external attacks. An IPS also makes it easier for the administrators to see where attacks are coming from so that they can address them and prevent any further attacks from that location [42]. An IPS device must use inspection to perform advanced protection against new types of attacks. It performs TCP segment reassembly, traffic analysis, application protocol validation, and signature matching to identify the attack [43].

A Host IPS solutions (HIPS) as shown in Figure 2.6 is designed to protect critical systems and applications by blocking attacks at the host and are considered the last line of defense, it can handle encrypted and unencrypted traffic equally, because it can analyze the data after it has been decrypted on the host [43].

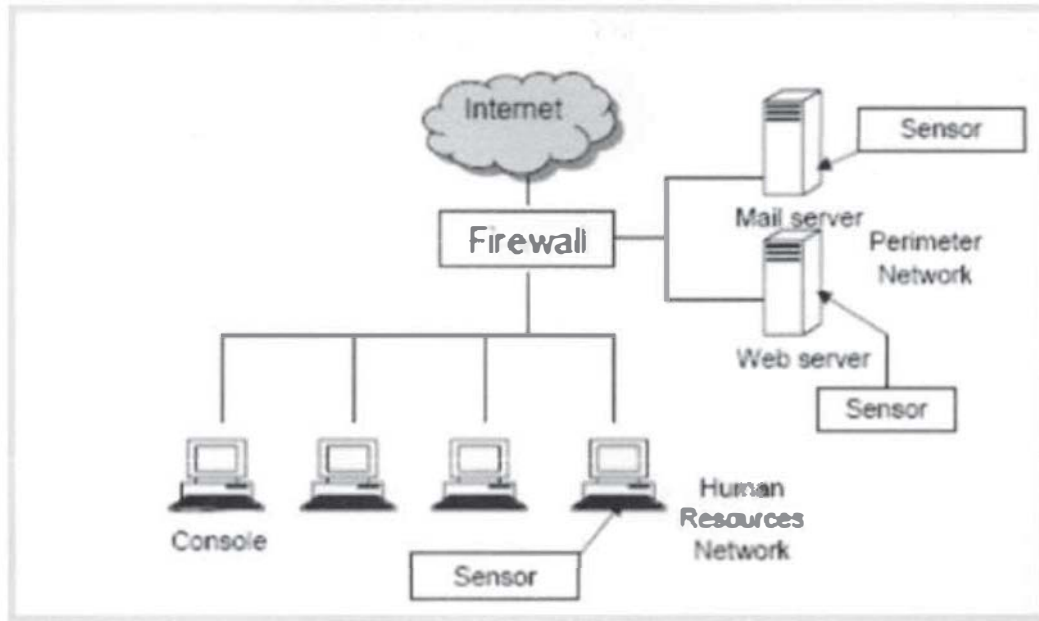


Figure 2. 6 A HIPS.

NIPS do not use processor and memory on computer hosts but uses its own CPU and memory. NIPS are a single point of failure, which is considered a disadvantage; however, this property also makes it simpler to maintain. However, this attribute applies to all network devices like routers and switches and can be overcome by implementing the network accordingly. NIPS can detect events scattered over the network and can react, whereas with a HIPS, only the host's data itself is available to make a decision. It would take too much time to report it to a central decision making engine and report back to block [44]. So, when we deploy both network and host IPS technologies they will provide the greatest level of protection for critical data and critical applications. Wireless intrusion prevention system (WIPS) prevent unauthorized network access to local area networks and other information assets by wireless devices [45].

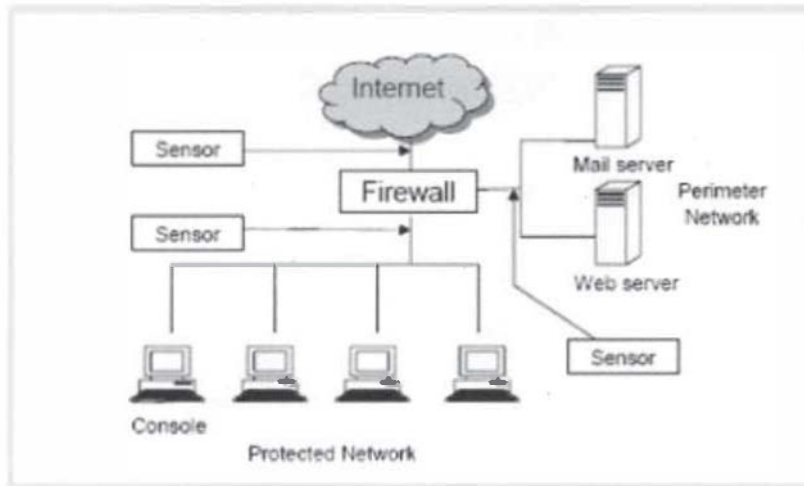


Figure 2. 7 A NIPS.

A Network IPS as shown in Figure 2.7, performs in-line inspection of network traffic in a near-real-time manner, the inspection identifies attacks using known vulnerabilities of commonly used software products and protocols, as well as known attack patterns with unusual activity based on connection sequences or traffic volume [42]. Intrusion Prevention Systems are considered extensions of Intrusion Detection Systems because both systems monitor network traffic and/or system activity for threats. The primary difference between the two systems is that Intrusion Prevention Systems are placed in-line and are therefore able to actively prevent/block intrusions that are detected. More specifically, an IPS can take such actions as sending an alarm, dropping malicious packets, resetting the connection and/or blocking traffic from an offending IP address. An IPS can also correct Cyclic Redundancy Check (CRC) errors, defragment packet streams, prevent TCP sequencing issues, and clean up unwanted transport and network layer options [40].

The deployment of an IPS is very effective technique to protect databases and networks from unauthorized users. It is used in many organizations to keep its own data secure. An IPS like any other development, it has some limitations and many advantages. Combining network

and host IPS technology results in the most comprehensive and robust defensive posture. Implementing and deploying proactive IPS technologies will result in fewer successful attacks, more efficient use of security resources, and lower operating costs than simply deploying a single, limited technology and hoping to avoid an attack. Combining IPS, IDS and Firewall technologies will provide a strong defense line to protect systems from any attack, for example firewall play as first defense line that connect to the second defense line IDS, and first and second lines connect to the third defense line IPS. Combining these three technologies will generate a great protection for any system. Generally an IPS is very useful when implemented in large networks [42].

## CHAPTER III

### METHODOLOGY

This chapter describes in details the methodology deployed in carrying out the objectives of this research. It is explained in a way that it can be easily reproduce if the need arises.

#### The Design Topology

Figure 3.1 shows this thesis's design topology, it consist of a layered approach using different vendor security devices to provide a defense in depth network perimeter security mechanism [46]. Network perimeter security should be designed to avoid a single point of failure. This design topology takes into account that by deploying different vendor security devices, an attack that could compromise one security device from a vendor might not be able to compromise other security device from other vendor. According to Conklin et al [46], the inadequacies of one security device could be complemented by other security devices from the whole architecture. Conklin also advocates that network security systems architecture should have the following layers;

- Routers
- Firewall
- Network segments referred to as perimeter security
- IDSs
- Encryption
- Authentication software
- Physical security and traffic control

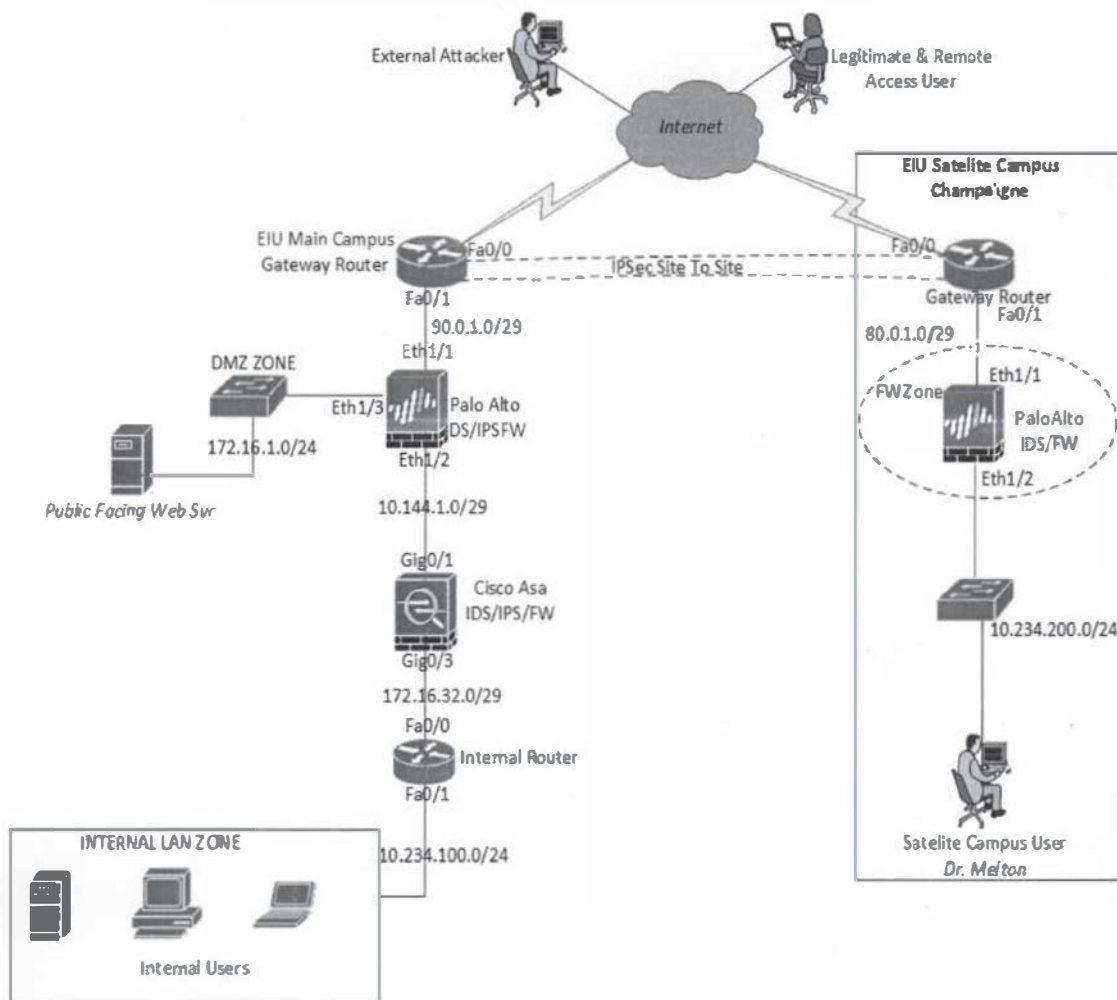


Figure 3. 1 The Topology for the Defense in Depth Network Perimeter Security for the EIU  
Cyber Security Lab

### The Router

In this research, a cisco router 2811 has been used. The cisco 2811 has the capacity to deliver secure data and great mobility. It comes with 2 integrated 10/100 fast Ethernet ports. In this research, the cisco router provide the following functions:

#### The EIU Main Computer Gateway Router

The EIU main campus gateway router in the design topology routes traffic into the designed network and processes traffic to the outside network when originated from the inside



network. As shown in Figure 3.1, the fast Ethernet 0/0 port is connected to an ISP that provides internet service for the designed lab. The interface is connected to a wireless bridge that connect wirelessly to the Verizon wireless hotspot for the purpose of internet access. The router fast Ethernet 0/0 port was configured as dynamic host configuration protocol (DHCP) client receiving IP address automatically from the Verizon wireless hotspot through the wireless bridge it is connected to. The IP address assigned by the Verizon hotspot is a private IP address in the range 192.168.1.0/24. A Public IP address is usually required to be able to route traffic to the internet. Since the IP address assigned is a private address, a Network Address Translation technique (NAT) is needed to translate the private IP address to a public address, this also serve as a form of security which protect the inside network IP address from being know to the outside network. The Verizon hotspot device provides this translation inbuilt, which means all traffic from the assigned private IP address will be translated to a public IP address. The NAT technique used by Verizon is Port Address Translation (PAT) which translate all the private assigned IP addresses in the range of 192.168.1.0/24 into a single public address to get to the internet. The router interface fast Ethernet 0/1 port was configured with the IP address 90.0.1.2/29, this interface connect directly to the Palo Alto firewall/IDS.

#### Port Translation to the Web Server

As shown in Figure 3.1, a webserver is placed in the DMZ zone of the network with an assigned private IP address 172.16.1.2/24. The private IP address will not allow external users to access this webserver. In order for external users to be able to access the webserver, the router is configured to have a public address representation for the webserver such that traffic sent to this public IP address will be translated to the private IP address of the webserver. In order for



the traffic originating from the outside or internet to successfully communicate with the webserver, the following process would have to take place;

1. The internet traffic destined to the webserver is first directed to the webserver's public IP address.
2. This traffic is then redirected to the router fast Ethernet 0/0 interface, this is made possible with the concept of port forwarding which was configured in the Verizon hotspot by directing all internet traffic to the router fast Ethernet 0/0 192.168.1.151 IP address as shown Figure 3.2.

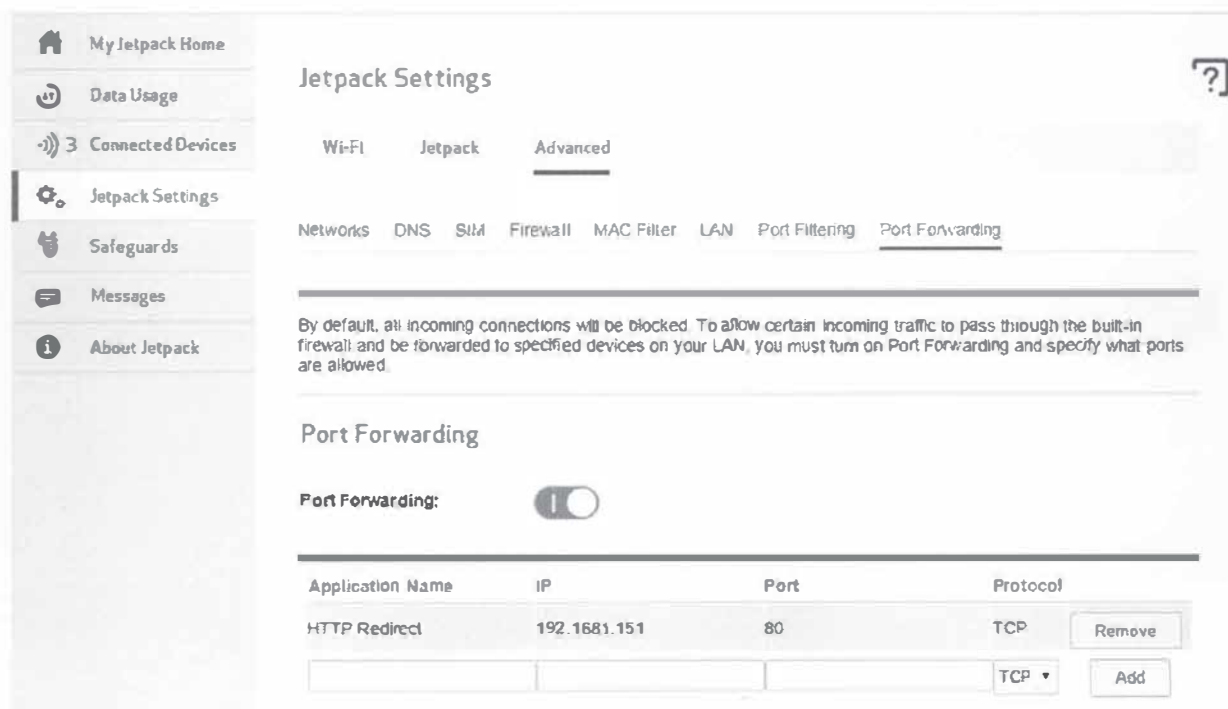


Figure 3. 2 Port forwarding configuration on the Verizon hotspot

When the traffic get redirected to the router fast Ethernet 0/0, the traffic is then further redirected to the web server. The explanation on how this is achieved will be provided as we proceed through the chapter.

## The Gateway Router NAT Configuration

In order for the traffic directed to the fast Ethernet 0/0 interface of the router to be redirected to the webserver, Network Address Translation is configured on the router. The IP address 192.168.1.151 on the fa0/0 interface is translated into the IP address 90.0.1.2 on interface fa0/1 which is directly connected to the Palo Alto firewall/IDS.

## The Palo Alto Firewall/IDS

In the design topology, a Palo Alto 200 (PA-200) device is used as second layer of security. A PA-200 has the capacity to function as a firewall as well as an intrusion detection system (IDS). It is capable of filtering/blocking malicious website or URL and also comes with denial of service mitigating features. The following configurations were done on the Palo Alto firewall device to achieve its purpose for this research.

## Interfaces and Zone Configuration

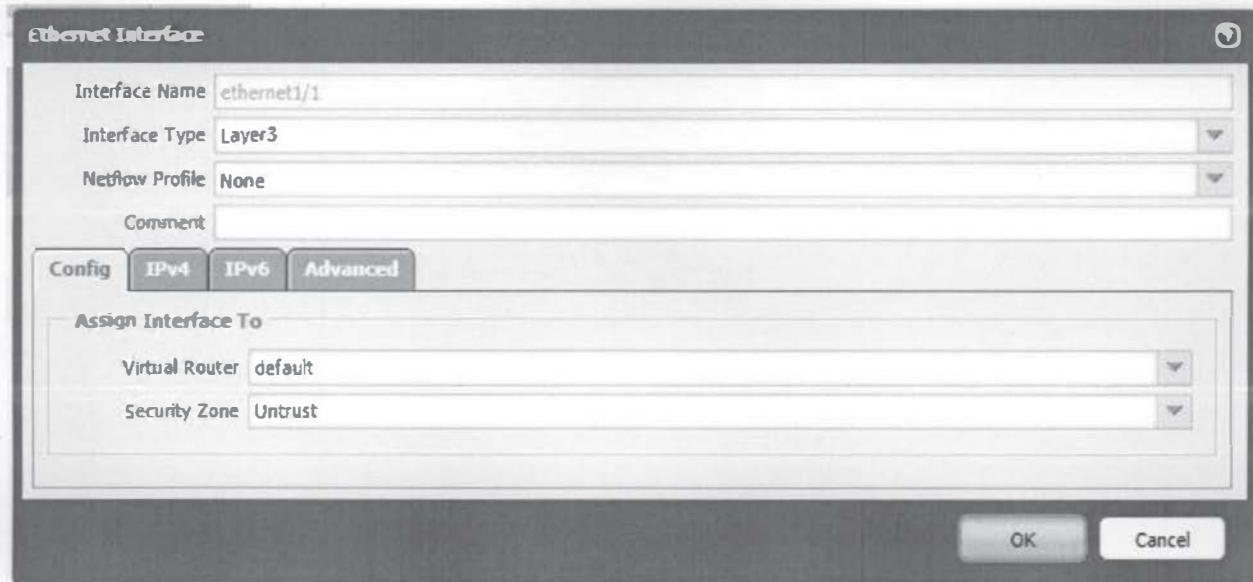
The Palo Alto device was configured with three different zones based on the design topology; the Trust Zone, the Untrusted Zone, and the DMZ Zone. The Ethernet interface 1/1 (E1/1) was configured as the Untrusted Zone which is connected to the gateway router, the Ethernet interface 1/2 (E1/2) was configured as the trusted zone, and Ethernet interface 1/3 (E1/3) was configured as the DMZ zone. The zones segmented the network and ensures that traffic going to a zone does not crosses to another zone. For example, when the webserver is placed at the DMZ zone, it ensures that traffic destined to it does not get to the trusted zone, this provide security for the internal users located in the trusted zone. The following steps explain how to configure the zones and the interfaces.

1. On the Palo Alto web administration portal, click on the Network Tab
2. Click on the zone tab on the left side pane

3. Click the add button to create a new zone as shown in Figure 3.3

Figure 3. 3 Creating a Zone

4. Name it, for example, DMZ and then select type as layer 3 and then click ok
5. Now to configure the interface, click the interface tab on the left hand side panel
6. Click on the interface to be configure, for example Ethernet 1/1, select the zone you want the interface to be associated with.



The screenshot shows the 'Ethernet Interface' configuration window. At the top, the title bar reads 'Ethernet Interface'. Below it, there are four input fields: 'Interface Name' with the value 'ethernet1/1', 'Interface Type' with a dropdown menu showing 'Layer3', 'Netflow Profile' with a dropdown menu showing 'None', and a 'Comment' text box. Below these fields are three tabs: 'Config', 'IPv4', 'IPv6', and 'Advanced'. The 'Config' tab is selected. Under the 'Config' tab, there is a section titled 'Assign Interface To' with two dropdown menus: 'Virtual Router' set to 'default' and 'Security Zone' set to 'Untrust'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Figure 3. 4 Interface configuration

7. Click on the IPv4 Tab

8. Click on add to configure IP address on the interface, then click OK



The screenshot shows the 'Ethernet Interface' configuration window with the 'IPv4' tab selected. The 'Type' section has three radio buttons: 'Static' (selected), 'PPPoE', and 'DHCP Client'. Below this is a table with one row for IP configuration. The table has a header 'IP' and a cell containing '90.0.1.1/29'. At the bottom of the table are '+ Add' and '- Delete' buttons. Below the table is a small text box with the placeholder 'IP address/netmask. Ex. 192.168.2.254/24'. At the bottom right of the window are 'OK' and 'Cancel' buttons.

Figure 3. 5 IP address configuration on the interface

9. Repeat the above steps to create the other zones and to configure other interfaces.

### Routing Configuration: Virtual Router

For the Palo Alto to route traffic from one zone to the other, it needs to understand how to route the traffic. Static routing is implemented and three static routes were configured: one of the static route routes traffic to any destination on the internet using the router fa0/1 interface IP address as the default gateway, the second static route routes traffic to the 172.16.32.0 network that is connected between the IDS/IPS device (Cisco ASA) and the internal router using ASA outside interface gig0/1 IP address as the default gateway and the third static route routes traffic to the 10.234.100.0/24 network using cisco ASA outside interface gig0/1 as the default gateway. The following steps show how to configure the static routes;

1. On the Palo Alto web administration portal, click on the Network Tab
2. Click on the Virtual Router tab on the left side panel as shown in Figure 3.6

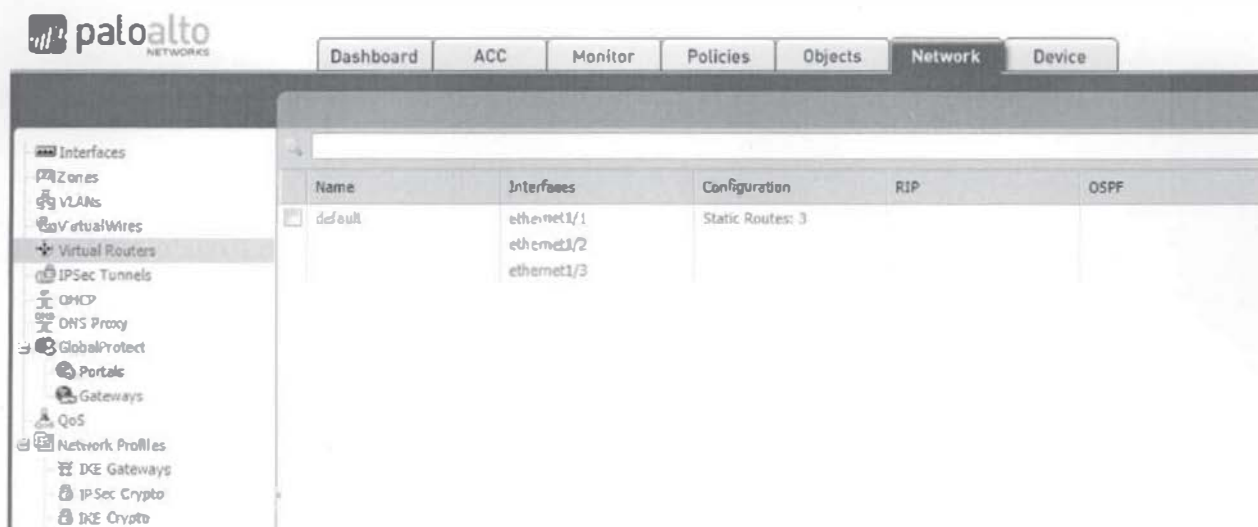


Figure 3. 6 Virtual Routers

3. Click add and give it a name as shown in Figure 3.7

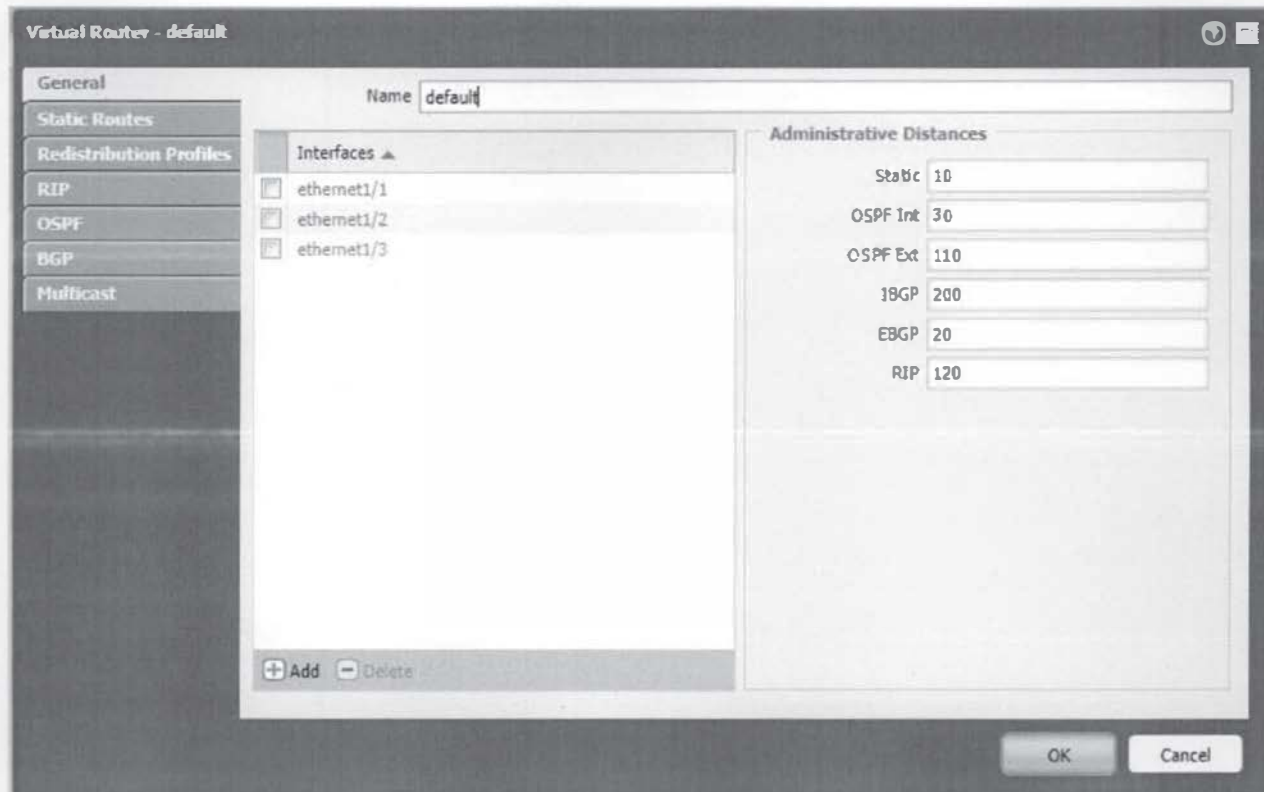


Figure 3. 7 Virtual Router Configuration

4. Click on static routes
5. Give your static route a name and configure the static route details as shown Figure 3.8
6. Then click ok.



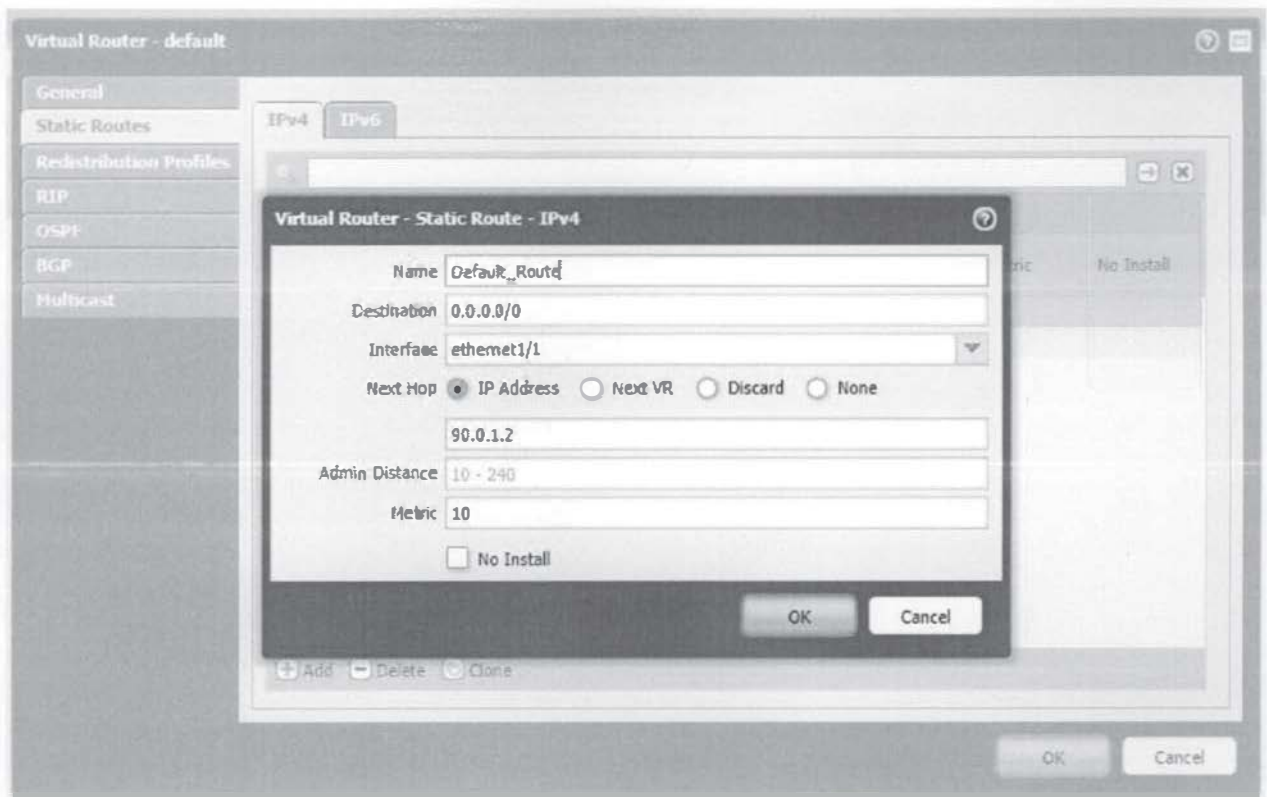


Figure 3. 8 Static Route configuration

Repeat all the steps above for the other static routes.

The virtual router has been created, now we need to attach the interfaces to the virtual router created.

7. Click on the interface tab on the left hand side of the panel and then click on an interface to edit it to attach it to the created virtual router as shown in Figure 3.9.

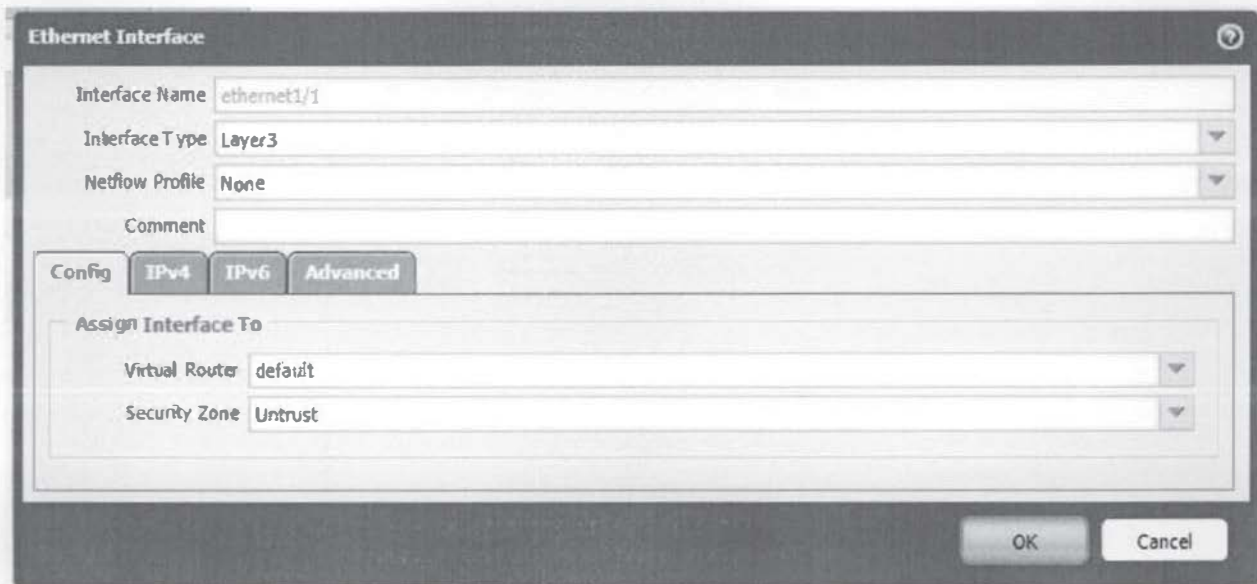


Figure 3. 9 Attaching an interface to a Virtual Router

### NAT Configuration and Security Policies

The Palo Alto was configured with a bidirectional NAT to translate the webserver IP address 172.16.1.2 to the IP address on the untrusted zone which is 90.0.1.1 when traffic is originating or returning from the webserver. Traffic from the internet destined to the webserver will first be translated to the gateway router interface fa0/0 which is 192.168.1.151 which also has been configured to redirect the traffic to the Palo Alto untrusted interface which is 90.0.1.1 and then it is port forwarded to the webserver.

Security policies was configured to allow or deny traffic between the zones. The following are the security policies configured as shown in Figure 3.10



Name	Tag	Zone	Address	User	HTTP Profile	Zone	Address	Application	Service	Action
Internet_Access	none	Trust	any	any	any	Untrust	any	any	any	Allow
OUT_DMZ	none	Untrust	any	any	any	DMZ	any	any	any	Allow
VPN	none	Untrust	VPN	any	any	Trust	LAN_Network	any	any	Allow
Allow_BI	none	Untrust	any	any	any	Trust	any	any	any	Allow
DMZ-UNT	none	DMZ	any	any	any	Untrust	any	any	any	Allow
DMZ_TRS	none	DMZ	any	any	any	Trust	any	any	any	Allow
TRIS_DMZ	none	Trust	any	any	any	DMZ	any	any	any	Allow

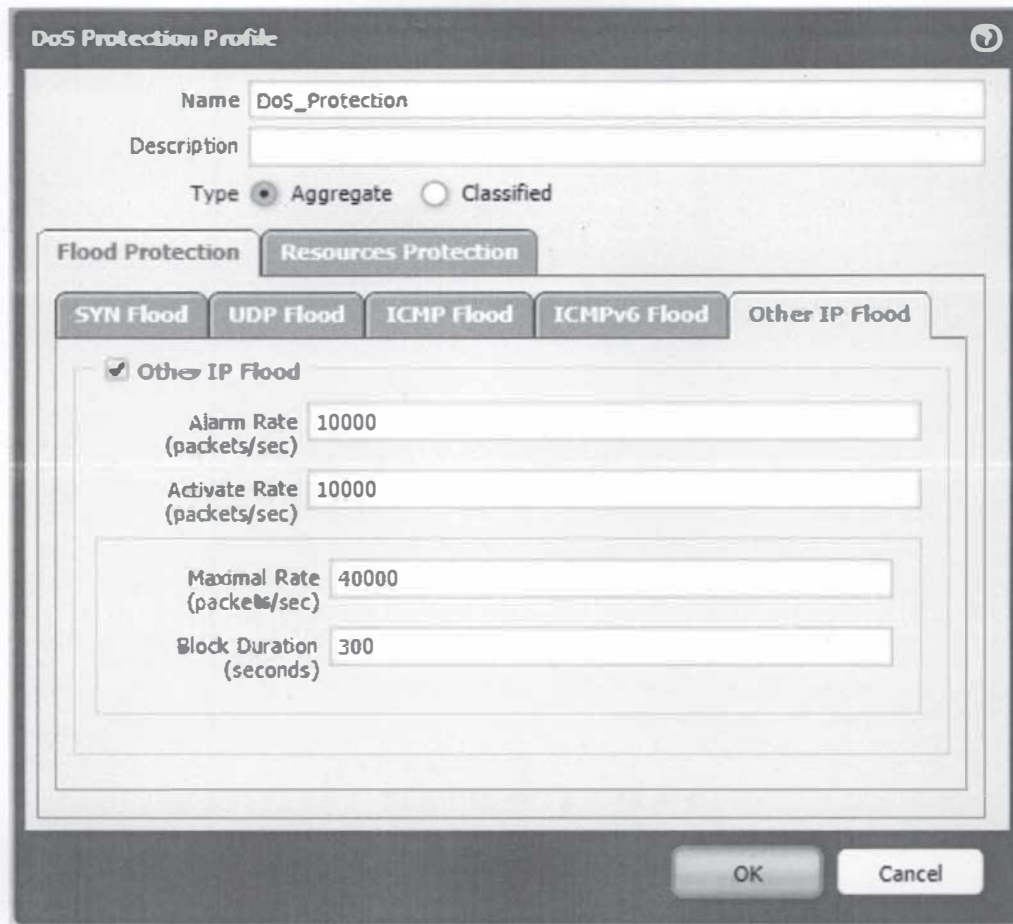
Figure 3. 10 Security Policies

All traffic that doesn't match these rules would be dropped.

#### Denial of Services (DoS) Protection Profile

The Palo Alto was also configured to mitigate against denial of service attack. The detail configuration steps is as follows;

1. On the Palo Alto web administration portal, click on the Object tab
2. Click the DoS protection tab
3. Click add
4. Name the DoS protection profile
5. Check the aggregate button to select it
6. Under the flood protection tab, check the buttons for SYN flood, UDP flood, ICMP flood and other IP flood tabs.
7. Click on resource protection tab and check the session button, then click OK.



The image shows a 'DoS Protection Profile' configuration window. At the top, the 'Name' field is set to 'DoS\_Protection'. Below it is an empty 'Description' field. The 'Type' is set to 'Aggregate' (selected with a radio button) and 'Classified' is unselected. There are two tabs: 'Flood Protection' and 'Resources Protection'. Under 'Flood Protection', there are five sub-tabs: 'SYN Flood', 'UDP Flood', 'ICMP Flood', 'ICMPv6 Flood', and 'Other IP Flood'. The 'Other IP Flood' sub-tab is selected, and its checkbox is checked. Inside this sub-tab, there are four input fields: 'Alarm Rate (packets/sec)' with value 10000, 'Activate Rate (packets/sec)' with value 10000, 'Maximal Rate (packets/sec)' with value 40000, and 'Block Duration (seconds)' with value 300. At the bottom right are 'OK' and 'Cancel' buttons.

Figure 3. 11 DoS Protection configuration

### Webserver Configuration

The webserver used for this research is hosted on a virtual machine running on Kali Linux Operating System. The system hosting the virtual machine is a core i7 Intel processor, with 8GB RAM and 1TB hard disk size with a windows server 2012 R2 Operating System. The webserver is configured with an IP address 172.16.1.2/24 and a vulnerable web application is installed on the webserver, it is the content of this webserver that loads whenever a request is made to the public webserver IP address.

### Cisco ASA Firewall Configuration and the Internal Router

The Cisco ASA firewall/IPS is a cisco 5512-x device that has an IPS sensor that comes with over 6000 signatures in its database. It is configured to allow traffic to flow from the inside and to the outside network while it is configured to block all other traffic. The interfaces has been configured to segment traffic flow.

Interface gig0/1 is connected to the Palo Alto and is configured as outside with a security level of 0, this means that traffic coming from this interface will not be trusted. Interface gig0/3 is connected to the internal router and is configured as inside with a security level of 100, this means traffic from this interface will be trusted. The ASA is configured to allow VPN traffic from the remote site to the Internal LAN network and also traffic from the inside network is allowed by default to go out to the internet.

The internal router is also a Cisco 2811 router just like the gateway router. The internal router serves as the gateway between the internal users and the outside network. It also serve as a point of security, filtering traffic by default and only configured traffic is allowed to cross the router interface network segment.

### The EIU Satellite Campus Gateway Router and the Firewall/IDS

As shown in Figure 3.12, the EIU satellite campus gateway router is a Cisco 2811 router and is configured similarly to the EIU main campus gateway router. The interface fast Ethernet 0/0 is connected to the wireless bridge and get an IP address through a dynamic host configuration protocol. The interface fast Ethernet 0/1 is connected directly to a Palo Alto firewall which also serves as an intrusion detection system. The interface fa0/1 is configured with an IP address of 80.0.1.2/29. Network address translation is also configured on it to allow the inside network to be able to reach the internet.

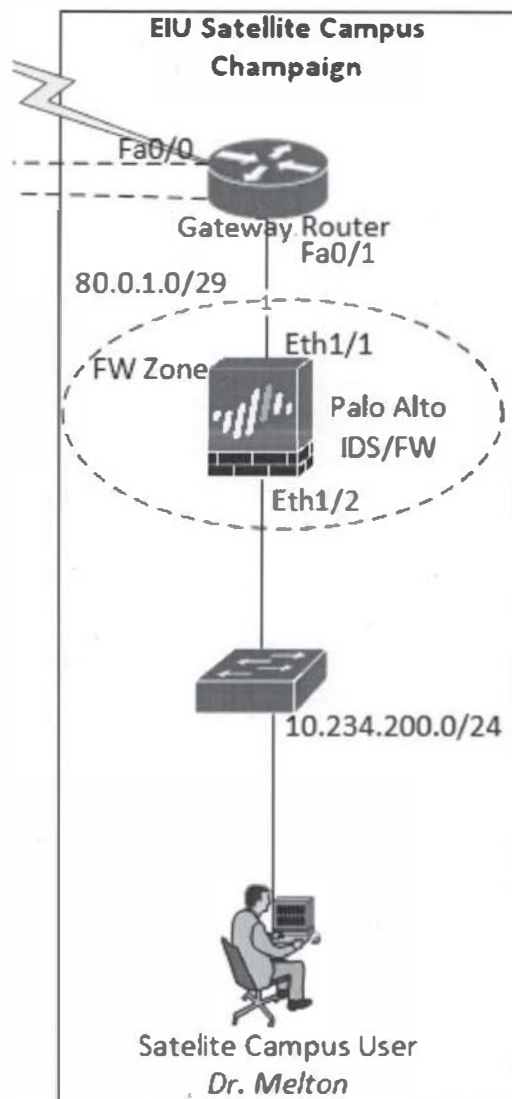


Figure 3. 12 EIU Satellite Campus Champaign

The EIU satellite campus firewall/IDS used is Palo Alto 200 same used in the EIU Main campus site as shown in Figure 3.12. Interface eth1/1 is configured as the untrusted zone while interface eth1/2 is configured as the trusted zone. Security policies such as allowing traffic to pass through from the trusted zone to the untrusted zone was also configured just like how it was configured on the EIU main campus Palo Alto as shown in the design topology.

## Virtual Private Network

As shown in the design topology, the main campus network is connected to the satellite campus network via IPSec Site to Site VPN. The VPN is terminated on the gateway routers on each sites. On each of the gateway routers, IPSec phase 1 is configured which defined the isakmp policies such as the authentication method which is a pre-share authentication method, hash algorithm, symmetric algorithm and the diffie hellman group. Then the pre-share key is defined and also the traffic to be protected is also defined which is the traffic from the main campus internal LAN network to the satellite campus internal LAN network and vice versa.

Then IPSec phase 2 is configured which defined the IPSec policies such as the encryption method, the tunnel mode. ESP encryption method is used while the default tunnel mode is used. The IPSec is applied to the interface connected to the ISP which is interface fa0/0 on both routers. Traffic from the main campus LAN network going to the satellite campus LAN network is being protected and vice versa traffic from the satellite campus network traffic to the main campus LAN network.

## CHAPTER IV

### RESULTS

This research has been able to achieve a major milestone in developing a laboratory for the Cyber Security program at EIU based on the available resources at the disposal as at the time of implementing this research. The research was able to simulate two sites connected over IPSec site to site VPN over the internet. The design has its own internet connection and makes it isolated from the EIU network. Internal LAN users are able to access the internet and can communicate with each other.

#### Results and Discussion

A major milestone in this research was that two simulated sites with real commercial equipment and a true internet connection were built and would serve as a test ground to launch cyber-attacks to each other. It will also serve to withstand attacks from the outsider or at least in the future record attacks to learn hacker's behavior. The sites can communicate to the internet and can also access each other through an IPsec site to site VPN. One of the vision of the cyber security program is to have a laboratory with two simulated sites which can be used to simulate cyber-attacks to each other for learning. This research has accomplished having this two sites implemented within the available resources. While this research could not go further with simulating cyber-attacks between each sites, connectivity between each sites was implemented and tested and it is hoped that further research in this project will dwell on this. Figure 4.1 and Figure 4.2 show the results of internal LAN users in EIU Main campus site and EIU Satellite Campus Champaign pinging [www.google.com](http://www.google.com) respectively proving that the internal users can access the external network on both sites.



```

Command Prompt

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::80e6:3db0:352e:98bf%8
    IPv4 Address. . . . . : 10.234.100.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.234.100.1

Ethernet adapter Ethernet 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter Local Area Connection* 3:

    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:0:9d38:6ab8:1c39:f129:595a:3468
    Link-local IPv6 Address . . . . . : fe80::1c39:f129:595a:3468%6
    Default Gateway . . . . . : ::

Tunnel adapter isatap.{6311A696-C843-438D-820E-8B318B781F8A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\GA Student>ping www.google.com

Pinging www.google.com [216.58.192.228] with 32 bytes of data:
Reply from 216.58.192.228: bytes=32 time=53ms TTL=47
Reply from 216.58.192.228: bytes=32 time=53ms TTL=47
Reply from 216.58.192.228: bytes=32 time=47ms TTL=47
Reply from 216.58.192.228: bytes=32 time=52ms TTL=47

Ping statistics for 216.58.192.228:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 47ms, Maximum = 53ms, Average = 51ms

C:\Users\GA Student>

```

Figure 4. 1 EIU Main Campus Internal LAN User (10.234.100.50/24) ping www.google.com

```
GA Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\GA Student>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 10.234.200.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.234.200.1

C:\Users\GA Student>ping www.google.com

Pinging www.google.com [172.217.6.4] with 32 bytes of data:
Reply from 172.217.6.4: bytes=32 time=43ms TTL=49
Reply from 172.217.6.4: bytes=32 time=48ms TTL=49
Reply from 172.217.6.4: bytes=32 time=44ms TTL=49
Reply from 172.217.6.4: bytes=32 time=58ms TTL=49

Ping statistics for 172.217.6.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 43ms, Maximum = 58ms, Average = 48ms

C:\Users\GA Student>
```

Figure 4. 2 EIU Satellite Campus Champaign Internal LAN User (10.234.200.50/24) ping

www.google.com

The Figure 4.3 shows EIU Internal LAN users accessing the webserver through the private address of the webserver (172.16.1.2).

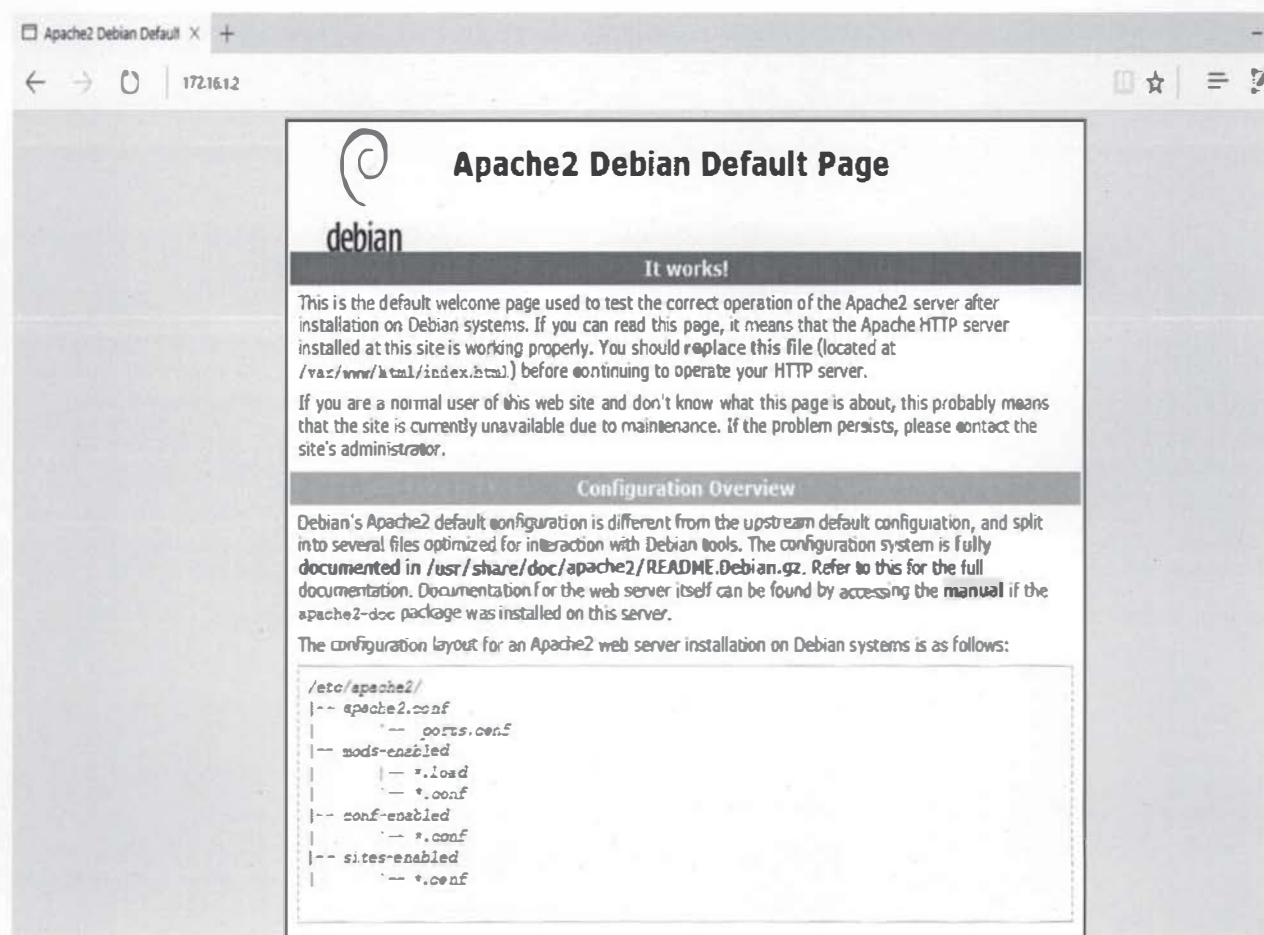


Figure 4. 3 EIU Main Campus Internal User accessing the Webserver through Private IP address  
172.16.1.2

The public IP address given by the ISP is 166.165.203.151. External users from the internet who want to access the webserver will be able to access the webserver through this IP address (166.165.203.151). As explained in chapter 3, this IP address will be redirected to the private IP address of the webserver in the DMZ zone. Figure 4.4 shows a successful web access from the internet to the webserver in the DMZ zone.

To test the VPN connectivity between the two sites, internal users in both sites will send pings to each other to test connectivity. The Figure 4.5 and Figure 4.6 shows successful ping connectivity between the two internal LAN users.



```

Command Prompt

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::80e6:3db0:352e:98bf%8
IPv4 Address. . . . . : 10.234.100.50
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.234.100.1

Ethernet adapter Ethernet 2:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

Tunnel adapter Local Area Connection* 3:

Connection-specific DNS Suffix . :
IPv6 Address. . . . . : 2001:0:9d38:6ab8:1c39:f129:595a:3468
Link-local IPv6 Address . . . . . : fe80::1c39:f129:595a:3468%6
Default Gateway . . . . . : ::

Tunnel adapter isatap.{6311A696-C843-438D-820E-8B318B781F8A}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\Users\GA Student>ping 10.234.200.50

Pinging 10.234.200.50 with 32 bytes of data:
Reply from 10.234.200.50: bytes=32 time=3ms TTL=123
Reply from 10.234.200.50: bytes=32 time=3ms TTL=123
Reply from 10.234.200.50: bytes=32 time=3ms TTL=123
Reply from 10.234.200.50: bytes=32 time=3ms TTL=123

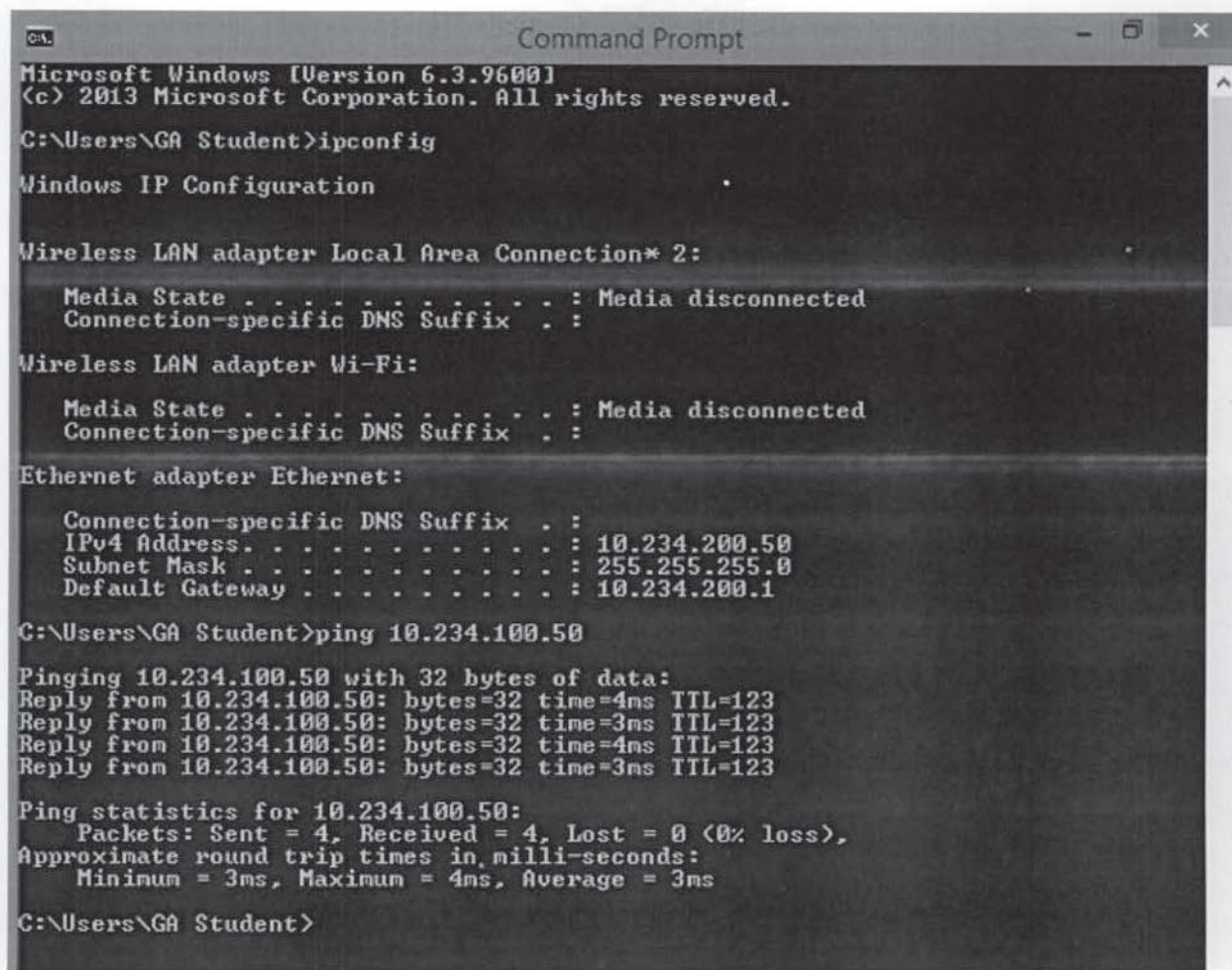
Ping statistics for 10.234.200.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\GA Student>

```

Figure 4. 5 EIU Main Campus Internal LAN User (10.234.100.50) pinging EIU Satellite Campus

Internal LAN user 10.234.200.50.



```

Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\GA Student>ipconfig

Windows IP Configuration

Wireless LAN adapter Local Area Connection* 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . :
    IPv4 Address. . . . . : 10.234.200.50
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.234.200.1

C:\Users\GA Student>ping 10.234.100.50

Pinging 10.234.100.50 with 32 bytes of data:
Reply from 10.234.100.50: bytes=32 time=4ms TTL=123
Reply from 10.234.100.50: bytes=32 time=3ms TTL=123
Reply from 10.234.100.50: bytes=32 time=4ms TTL=123
Reply from 10.234.100.50: bytes=32 time=3ms TTL=123

Ping statistics for 10.234.100.50:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 4ms, Average = 3ms

C:\Users\GA Student>

```

Figure 4. 6 EIU Satellite Campus Internal LAN User (10.234.200.50) pinging EIU Main Campus Internal LAN user 10.234.100.50.

### Conclusion

The main purpose of this research is to develop a design topology that can be used for laboratory practices for the cyber security program at EIU. The research fulfill this purpose by building two remote sites which can be used to simulate cyber-attacks. Also the publicly access webserver would also serve to invite hackers to hack into and serve to teach students the various hackers bypass security firewall. Inside users can also use the webserver to test internal hacking. The design developed would be a practical complement to the cyber security theoretical knowledge studied in the class.



### Recommendation

In line with the primary focus of this designed topology, it is recommended that future work on this research should focus more on cyber-attacks simulations of the design topology between the two sites and also from the external source such as hackers from the internet. It is also my recommendation that licenses of the security devices should be updated to aid the cyber-attack simulation. Modification can be done on the designed topology to further advance the design and implementation.

More importantly, I strongly recommend a complimentary virtual environment to simulate the designed topology and other laboratory practices for the cyber security practical learning. In the course of the research and within the available resources at the disposal of the department, I recommend GNS3 emulator software. Further research can be carried out on how this can be deploy but it is realistically possible to implement without any issue of software image with cisco or Palo Alto.

The following technology objectives could not be achieve as a result of the available resources;

- Network Device High Available: The license on the Cisco ASA would be need to be upgrade to security plus to achieve this. With the GNS3 emulator this can be easily achieve.
- Remote Access VPN: The software version of the device used for the gateway router could not accommodate the client VPN image due to low flash space. This can be upgraded or a mode advanced router could be use.

## REFERENCES

- [1] Hirschmann, Joerg, "Defense in Depth: A Layered Approach to Network Security". *Security: Solutions for Enterprise Security Leaders*, 51(9), 95-95, 2014.
- [2] Center for strategic and International studies. "Net Losses: Estimating the Global Cost of Cybercrime", 2014[online]. Available: <https://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf>. [Accessed: 21-Nov-2015].
- [3] Z. Lenny *et al.*, "Inside Network Perimeter Security", 2005, pp. 22.
- [4] N. Waisman *et al.*, "Methods and Apparatus for computer Network Security using Intrusion Detection and Prevention". US Patent 7225468 B2, May 29, 2007.
- [5] Johnson, Johna Till, "Security today means playing 'defense-in-depth' ", *Network World*, 21(33), 24-24.
- [6] Computer Security Institute. "CSI/FBI Computer Crime and Security Survey". Retrieved from <http://www.firenetltd.it/materiale/FBI2003.pdf>
- [7] Hendry, R. Erica, "How the Equifax hacked happened, according to its CEO". Retrieved from <http://www.pbs.org/newshour/rundown/equifax-hack-happened-according-ceo>
- [8] M. Riley and J. Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known". Retrieved from <https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections>
- [9] Selena Larson, "Every single Yahoo account was hacked – 3 billion in all". Retrieved from <http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html>
- [10] N. Spring, "Cyber Security: Are We Doing Enough"? (Cover story). *Electric Light & Power*, 86(3), 20-26, 2008.

- [11] Ray Lapena, "Tripwire Study: 75 Percent of Organizations Lack Skilled Cyber Security Experts". Retrieved from <https://www.tripwire.com/company/press-releases/2016/10/tripwire-study-75-percent-of-organizations-lack-skilled-cyber-security-experts/>
- [12] J. A. Chisholm, "Analysis on the Perceived Usefulness of Hands-on Virtual Labs in Cybersecurity Classes", 2015.
- [13] C. Folk, D. Hurley, W. K. Kaplow, J. F. X. Payne, "The Security implications of The Internet of Things". Retrieved from <https://www.mitre.org/sites/default/files/publications/afcea-white-paper-security-implications-internet-of-things.pdf>, 2015
- [14] M. S. Zareen, M. Akhlaq, M. Tariq, U. Khalid, "2013 2nd National Conference on Information Assurance", 2013
- [15] D. Millier, "How cyber security works". Retrieved from <http://www.uzado.com/blog/how-cyber-security-works>, 2017
- [16] S. Larson, "The Hack that left exposed in 2017". Retrieved from <http://money.cnn.com/2017/12/18/technology/biggest-cyberattacks-of-the-year/index.html>, 2017
- [17] M. Nunnikhoven, "Cloud Security: To patch or not to patch". Retrieved from <https://blog.trendmicro.com/cloud-security-to-patch-or-not-to-patch/>, 2015
- [18] P. H. O'Neil, "Ransomware is now a \$2 billion-per-year criminal industry". Retrieved from <https://www.cyberscoop.com/ransomware-2-billion-hitdefender-gpu-encryption/>, 2017
- [19] N. Ismail, "10 of the biggest hack that rock the business world in 2017". Retrieved from <http://www.information-age.com/10-biggest-hacks-rocked-business-world-2017-123469857/>, 2017

- [20]S. Larson, "Data of almost 200 million voters leaked online by GOP analytics firm".  
Retrieved from <http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html?iid=EL>, 2017
- [21]Cisco Systems, "What is a VPN". Retrieved from  
<https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html>
- [22]Wikimedia Commons, "File:Virtual Private Network Overview". Retrieved from  
[https://commons.wikimdeaia.org/wiki/File:Virtual\\_Private\\_Network\\_overview.svg](https://commons.wikimdeaia.org/wiki/File:Virtual_Private_Network_overview.svg)
- [22]B. Nouredine, "Security of mobile communications", CRC Press, pp. 32-33, 2010.
- [23]O. Rolf, "Internet Security: Firewalls and Beyond", Communications of the ACM, vol. 5, no. 40, pp. 94, 1997.
- [24]W. R. Cheswick and S. M. Belovin, "Firewalls and Internet Security, Repelling the Wily Hacker", Addison-Wesley Publishing Company, 1994.
- [25]M. Mohit, R. Kumar, A. Bharti, J. Kishan, "Intrusion Detection Systems", International Journal of Technical Research and Applications, vol. 5, No. 2, pp. 38-44, 2017.
- [26]S. Vijayarani and M. Sylviaa, "Intrusion Detection System", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol.4, No. 1, 2015.
- [27]J. P. Anderson, "Computer Security Threat Monitoring and Surveillance", Retrieved from  
<http://csrc.nist.gov/publications/history/#ande80>, 1980.
- [28]H. Debar, M. Dacier, A. Wespi, "Towards a taxonomy of Intrusion Detection Systems",  
Retrieved from <http://perso.rd.francetelecom.fr/debar/papers/DebDacWes99.pdf>

- [29]B. S. Kumar, T. C. Raju, M. Ratnakar, S. K. Baba, N. Sudhakar, "Intrusion Detection System-Types and Prevention", International Journal of Computer Science and Information Technologies, Vol. 4, No. 1, pp. 77-82, 2013.
- [30]B. Rebecca, "An introduction to Intrusion Detection & Assessment", ICSA, 2009.
- [31]R. G. Bace, "Intrusion Detection", Macmillan Technical Publishing, 2000.
- [32]D. E. Denning, "An Intrusion Detection Model", Proceedings of the Seventh IEEE Symposium on Security and Privacy, 1986.
- [33]ICSA, "Intrusion Detection System Buyer's Guide", Retrieved from <https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf>, 1998
- [34]K. R. Karthikeyan, A. Indra, "Intrusion Detection Tools and Techniques Survey", International Journal of Computer Theory and Engineering, Vol.2, No.6, pp. 1793-8201, 2010.
- [35]J. Blanchard, "SANS Penetration Testing", Retrieved from <https://pen-testing.sans.org/blog/2017/12/12/sans-poster-building-a-better-pen-tester-pdf-download?msc=PTslider>, 2017.
- [36]D. Lulzsec, "Disbands: The Attacks Live On", Infosec Island, 2011.
- [37]K. Kane, "IBM and Ponema Institute: Cost of Data Breach dropped by 10 percent globally in 2017 study", Retrieved from <https://www.prnewswire.com/news-releases/ibm--ponemon-institute-cost-of-a-data-breach-dropped-10-percent-globally-in-2017-study-300476378.html>, 2017
- [38]E. Amoroso, "Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response", Intrusion.Net Books, 1999.

- [39]A. A. Abdelkarim, H. H. Nasereddin, "Intrusion Prevention System", International Journal of Academic Research, Vol. 3, No. 1, 2011.
- [40]D. Neil, "Intrusion Prevention Systems: The Next Step in the Evolution of IDS", Retrieved from <http://www.securityfocus.com/infocus/1670>, 2018.
- [41]P. Mell, K. Kent, J. Nusbaum, "Guide to Malware Incident Prevention and Handling", National Institute of Standards and Technology, 2005.
- [42]MCAFEE, "Network Intrusion Prevention Systems Justification and ROI", Retrieved from [https://usacac.army.mil/cac2/cew/repository/papers/Network\\_Intrusion.pdf](https://usacac.army.mil/cac2/cew/repository/papers/Network_Intrusion.pdf), 2004
- [43]R. C. Newman, "Computer Security: Protecting Digital Resources", Jones and Bartlett Publishers, 2010.
- [44]M. E. Whitman, H. J. Mattord, "Principles of Information Security", Cengage Learning EMEA, 2009.
- [45]P. Helman, G. Liepins, W. Richards, "Foundation of Intrusion Detection In Proceedings of IEEE Computer Security Foundation Workshops", IEEE Computer Security Foundations Workshop V, 1992.
- [46]W. Conklin, G. White, D. Williams, R. Davis and C. Cothren, "Principle of computer security, 2016.



## APPENDICES

Appendix A: Definition of terms

Appendix B: Configuration of EIU Main Gateway Router

Appendix C: Configuration of Cisco ASA Firewall

Appendix D: Configuration of Internal Router

Appendix E: Configuration of EIU Satellite Campus Gateway Router

Appendix F: Laboratory Guidelines

## Appendix A – Definition of Terms

**Cybersecurity:** Cybersecurity is the practice of protecting systems, networks and programs from digital attacks. These attacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.

**Demilitarized Zone (DMZ):** A DMZ; sometimes referred to as a perimeter network is a physical or logical subnetwork that contains and exposes an organization's external facing services to an unsecure untrusted large network such as internet.

**Firewall:** Is a network device hardware, software, or a combination thereof whose purpose is to enforce a security policy across its connections by allowing or denying traffic to pass into or out of the network.

**Intrusion Detection System (IDS):** An intrusion detection system is a system that detects malicious activity on a computer or network. It only detect and not prevent malicious activity.

**Intrusion Prevention System (IPS):** An intrusion prevention system monitor network traffic for malicious activities and when it detect a malicious activity it blocks it based on the configuration.

**Local Area Network (LAN):** A local area network is a group of computers and associated devices that connect together within a close proximity to each other.

**Virtual Private Network (VPN):** A VPN is a technology that creates an encrypted connection over an unsecure network.

## Appendix B – Configuration of EIU Main Gateway Router

EIU\_Main\_Campus#sh run

Building configuration...

Current configuration : 2015 bytes

!

! Last configuration change at 19:36:34 UTC Fri Mar 9 2018

version 15.1

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname EIU\_Main\_Campus

!

boot-start-marker

boot-end-marker

!

no aaa new-model

!

dot11 syslog

ip source-route

!

ip cef

!

multilink bundle-name authenticated

!

crypto pki token default removal timeout 0

!

license udi pid CISCO2811 sn FTX1040A2F0

!

redundancy

!

ip ftp username ben

ip ftp password password

!

crypto isakmp policy 10

encr aes

hash md5

authentication pre-share

group 2

crypto isakmp key cisco address 192.168.1.211

!

crypto ipsec transform-set MYTHESIS esp-aes esp-sha-hmac

!

crypto map MYMAP 10 ipsec-isakmp

```
set peer 192.168.1.211
set transform-set MYTHESIS
match address VPN
!
interface FastEthernet0/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map MYMAP
!
interface FastEthernet0/1
 ip address 90.0.1.2 255.255.255.248
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
interface FastEthernet0/0/0
 no ip address
!
interface FastEthernet0/0/1
 no ip address
!
interface FastEthernet0/0/2
 no ip address
!
interface FastEthernet0/0/3
 no ip address
!
interface Vlan1
 no ip address
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 105 interface FastEthernet0/0 overload
ip nat inside source static tcp 90.0.1.1 80 192.168.1.151 80 extendable
ip route 10.144.1.0 255.255.255.248 90.0.1.1
ip route 10.234.100.0 255.255.255.0 90.0.1.1
ip route 10.234.200.0 255.255.255.0 192.168.1.211
ip route 172.16.32.0 255.255.255.248 90.0.1.1
!
ip access-list extended VPN
```

```
permit ip 10.234.100.0 0.0.0.255 10.234.200.0 0.0.0.255
!  
access-list 105 deny ip 10.234.100.0 0.0.0.255 10.234.200.0 0.0.0.255  
access-list 105 permit ip any any  
!  
control-plane  
!  
line con 0  
line aux 0  
line vty 0 4  
login  
transport input all  
!  
scheduler allocate 20000 1000  
end
```

## Appendix C – Configuration of Cisco ASA Firewall

```
ASA-FW-IPS# sh run
: Saved
:
ASA Version 9.1(2)
!
hostname ASA-FW-IPS
enable password E.bgA9kfttKB/.vi encrypted
names
!
interface GigabitEthernet0/0
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/1
nameif Outside
security-level 0
ip address 10.144.1.1 255.255.255.248
!
interface GigabitEthernet0/2
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/3
nameif Inside
security-level 100
ip address 172.16.32.2 255.255.255.248
!
interface GigabitEthernet0/4
shutdown
no nameif
no security-level
no ip address
!
interface GigabitEthernet0/5
shutdown
no nameif
no security-level
no ip address
!
interface Management0/0
```



```

management-only
shutdown
no nameif
no security-level
no ip address
!
ftp mode passive
access-list OUT-IN extended permit ip 10.234.200.0 255.255.255.0 10.234.100.0 255.255.255.0
access-list OUT-IN extended permit ip 172.16.1.0 255.255.255.0 10.234.100.0 255.255.255.0
access-list OUT-IN extended permit icmp 90.0.1.0 255.255.255.248 any
access-list OUT-IN extended permit icmp 172.16.1.0 255.255.255.0 any
pager lines 24
mtu Outside 1500
mtu Inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
access-group OUT-IN in interface Outside
route Outside 0.0.0.0 0.0.0.0 10.144.1.2 1
route Inside 10.234.100.0 255.255.255.0 172.16.32.1 1
route Outside 172.16.1.0 255.255.255.0 10.144.1.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec security-association pmtu-aging infinite
crypto ca trustpool policy
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default

```

```
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect http
!
service-policy global_policy global
prompt hostname context
call-home reporting anonymous prompt 2
Cryptochecksum:954e4ed0d555296be604bb44f4f0012d
: end
```

## Appendix D – Configuration of Internal Router

Internal-Router#sh run  
Building configuration...

Current configuration : 1404 bytes

```
!  
version 15.1  
service timestamps debug datetime msec  
service timestamps log datetime msec  
no service password-encryption  
!  
hostname Internal-Router  
!  
boot-start-marker  
boot-end-marker  
!  
no aaa new-model  
!  
dot11 syslog  
ip source-route  
!  
ip cef  
!  
multilink bundle-name authenticated  
!  
crypto pki token default removal timeout 0  
!  
license udi pid CISCO2811 sn FTX1040A2ET  
username cisco password 0 cisco  
!  
redundancy  
!  
interface FastEthernet0/0  
description Outside Interface  
ip address 172.16.32.1 255.255.255.248  
ip nat outside  
ip virtual-reassembly in  
duplex auto  
speed auto  
!  
interface FastEthernet0/1  
description Inside Interface  
ip address 10.234.100.1 255.255.255.0  
ip nat inside  
ip virtual-reassembly in
```

```
duplex auto
speed auto
!
interface FastEthernet0/0/0
no ip address
!
interface FastEthernet0/0/1
no ip address
!
interface FastEthernet0/0/2
no ip address
!
interface FastEthernet0/0/3
no ip address
!
interface Vlan1
no ip address
!
ip forward-protocol nd
ip http server
ip http authentication local
no ip http secure-server
!
!
ip route 0.0.0.0 0.0.0.0 172.16.32.2
ip route 10.144.1.0 255.255.255.248 172.16.32.2
ip route 90.0.1.0 255.255.255.248 172.16.32.2
ip route 172.16.1.0 255.255.255.248 172.16.32.2
!
control-plane
!
line con 0
line aux 0
line vty 0 4
login
transport input all
!
scheduler allocate 20000 1000
end
```

## Appendix E – Configuration of EIU Satellite Campus Gateway Router

Champaign\_GatewayRouter#sh run  
Building configuration...

Current configuration: 3609 bytes

```
!
version 15.1
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Champaigne_GatewayRouter
!
boot-start-marker
boot-end-marker
!
enable password cisco
!
no aaa new-model
!
dot11 syslog
ip source-route
!
ip cef
!
multilink bundle-name authenticated
!
crypto pki token default removal timeout 0
!
crypto pki trustpoint TP-self-signed-213188813
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-213188813
  revocation-check none
  rsa-keypair TP-self-signed-213188813
!
crypto pki certificate chain TP-self-signed-213188813
  certificate self-signed 01
    30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
    30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
    69666963 6174652D 32313331 38383831 33301E17 0D313631 30303832 31323132
    365A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
    532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3231 33313838
    38313330 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
    AE9D3C81 0DB757DA BAF9C235 9208D06E 0C0055A7 42639BD0 DEDE2A33
    A7D235FC
```

```

0ECC8431 C69847B1 FA0596DA EDEBEDD1 8DC17C74 2846C614 2C807B16 69B58A05
5BD2EECE 6E2BE599 6E15AF65 00B8A3F6 867CF508 F6B33CAB 7D24D155 D4FAAA97
07A68D32 4C0C18B2 735FA9F0 C6C935A7 35C12D2E 1981FB2E 70B47533 1CD01365
02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
23041830 1680147E 2012F70C 4DE3A977 904E3BB5 C408C040 31D48F30 1D060355
1D0E0416 04147E20 12F70C4D E3A97790 4E3BB5C4 08C04031 D48F300D 06092A86
4886F70D 01010505 00038181 0042220E ADD17AB1 32B4A3A0 132D8F38 05ACF25D
AD9E2380 7FCD6D6F 037A97EA 44A6E416 12B4BDB6 18D16C75 B5588299 68096AE9
9B45AAD0 2A77C885 954F6DA1 04A32B9D 43D2C617 297ED254 EC804450 F5931B36
370711FB E024CD11 D1CE9421 8E04BA22 D799D253 EC5D8EC6 7E537C1B EE78F609
2D2FCC58 B04E6CED 9E8548A4 24

```

quit

```

!
license udi pid CISCO2811 sn FTX1040A2F3
username cisco privilege 15 password 0 cisco

```

```

!
redundancy

```

```

!
crypto isakmp policy 10
set peer 192.168.1.151
set transform-set MYTHESIS
match address VPN

```

```

!
interface FastEthernet0/0
ip address dhcp
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
crypto map MYMAP

```

```

!
interface FastEthernet0/1
ip address 80.0.1.2 255.255.255.248
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto

```

```

!
interface FastEthernet0/0/0
no ip address

```

```

!
interface FastEthernet0/0/1
no ip address

```

```

!
interface FastEthernet0/0/2
no ip address

```



```
!  
interface FastEthernet0/0/3  
no ip address  
!  
interface Vlan1  
no ip address  
!  
ip forward-protocol nd  
ip http server  
ip http authentication local  
ip http secure-server  
!  
ip nat inside source list NAT interface FastEthernet0/0 overload  
ip route 0.0.0.0 0.0.0.0 192.168.1.1  
ip route 10.234.100.0 255.255.255.0 192.168.1.151  
ip route 10.234.200.0 255.255.255.0 80.0.1.1  
!  
ip access-list extended NAT  
deny ip 10.234.200.0 0.0.0.255 10.234.100.0 0.0.0.255  
permit ip 10.234.200.0 0.0.0.255 any  
ip access-list extended VPN  
permit ip 10.234.200.0 0.0.0.255 10.234.100.0 0.0.0.255  
!  
no cdp run  
!  
control-plane  
!  
line con 0  
line aux 0  
line vty 0 4  
privilege level 15  
password cisco  
login local  
transport input telnet ssh  
line vty 5 15  
password cisco  
login local  
transport input all  
!  
scheduler allocate 20000 1000  
end
```

## Appendix F – Laboratory Guidelines

### NETWORK SECURITY

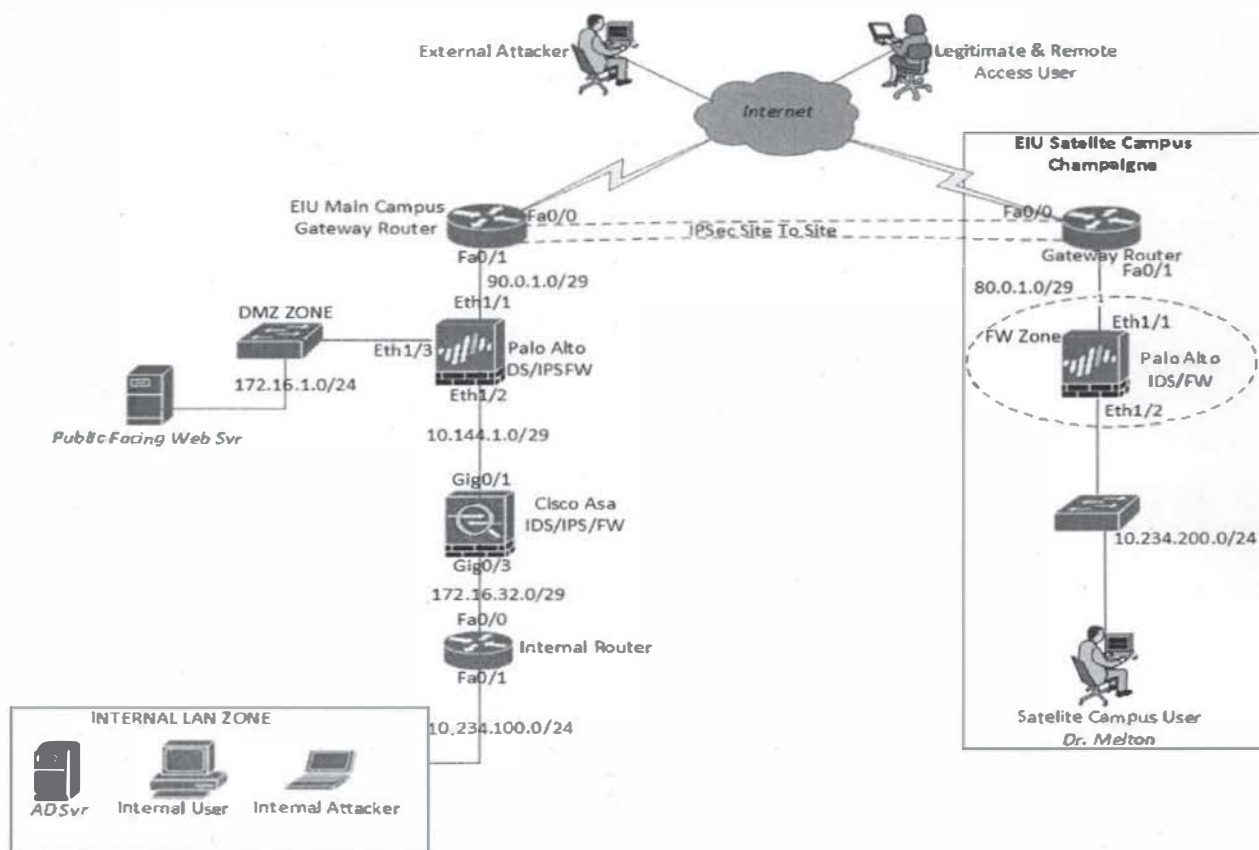
#### LABORATORY I: BUILDING THE NETWORK

**Lab Purpose:** The purpose of this lab exercise is to introduce students to different network security devices by having access to the network device and configuring the network device ip addresses. Configuring the IP addresses of the network devices will expose students to some basic command lines and serve as a start to their introduction to different network security devices.

**Assumption:** It is assumed that students have some basic knowledge in networking.

**Task:**

The network topology below has been physically connected, configure and assign ip addresses to interfaces of the network devices.



### Solution Guide

**NOTE:** You need to connect a management computer to the console of the router to have access to the command line interface of the router.

- EIU Main Campus Gateway Router  
 EIU\_Main\_Campus>enable  
 EIU\_Main\_Campus#Conf t  
 EIU\_Main\_Campus(config)#int fa0/0  
 EIU\_Main\_Campus(config-if)#ip address dhcp  
 EIU\_Main\_Campus(config-if)#no shutdown  
 EIU\_Main\_Campus(config)#ex it  
 EIU\_Main\_Campus(config)#int fa0/1  
 EIU\_Main\_Campus(config-if)#ip address 90.0.1.2 255.255.255.248  
 EIU\_Main\_Campus(config-if)#no shutdown

- Palo Alto

You will need to connect physically to the management port of the Palo Alto and configure your system IP address as follow:

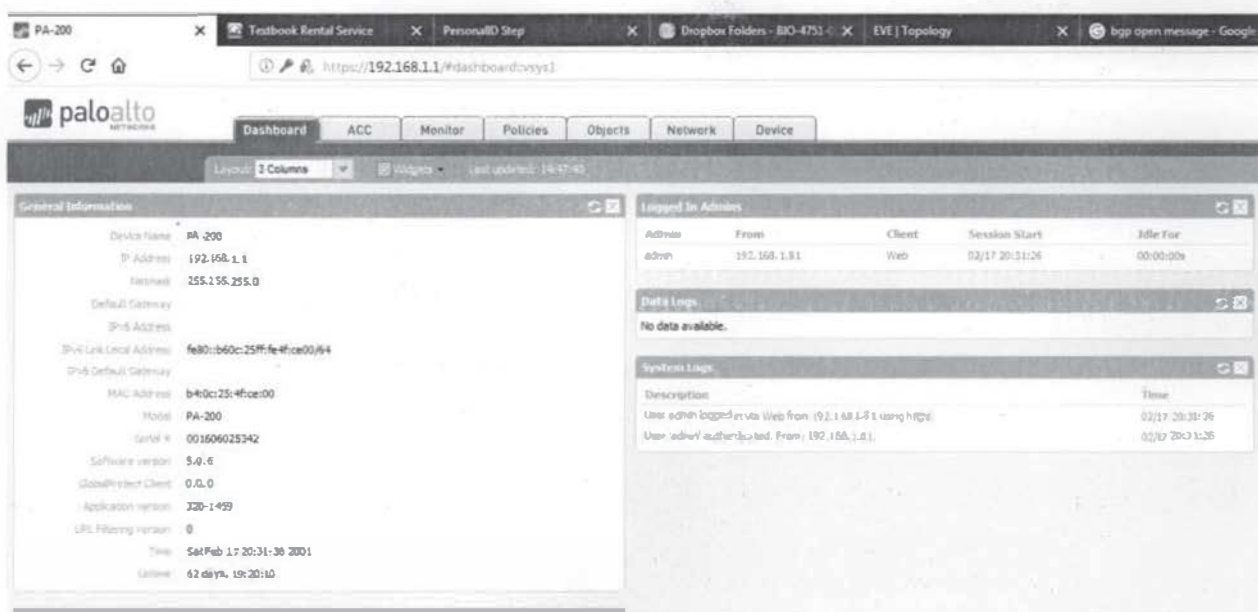
Your System IP address: 192.168.1.2 and subnet mask of 255.255.255.0

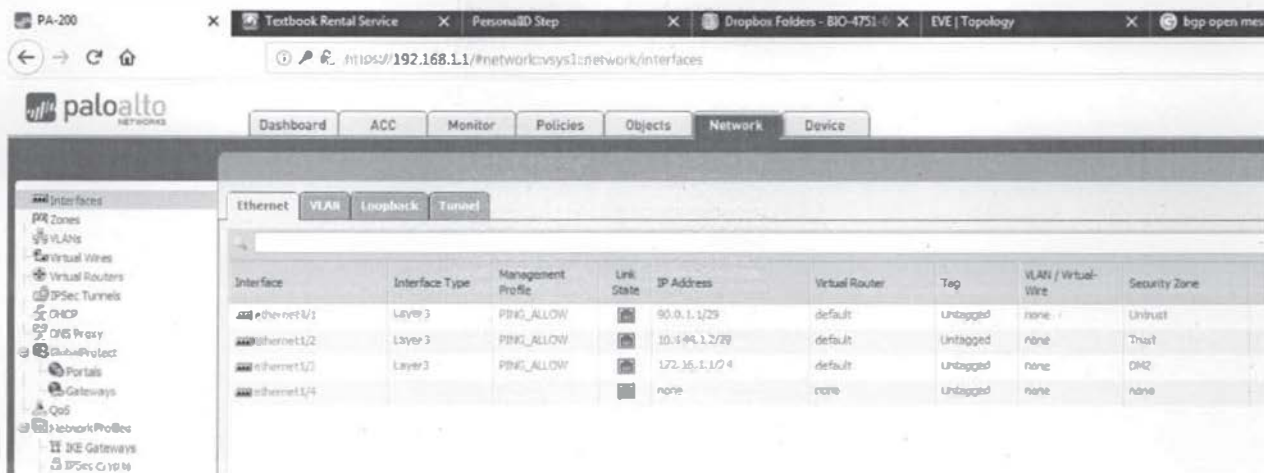
Then go to <https://192.168.1.1> on your browser to access Palo Alto Web Portal.

Username/Password is admin/admin

The web page will appear as this:

Configure the interface as shown below.





## - Cisco ASA

```
ASA-FW-IPS#conf t
ASA-FW-IPS(config)#int gig0/1
ASA-FW-IPS(config-if)#nameif Outside
ASA-FW-IPS(config-if)#security-level 0
ASA-FW-IPS(config-if)#ip address 10.144.1.1 255.255.255.248
ASA-FW-IPS(config-if)#no shutdown
ASA-FW-IPS(config-if)#exit
ASA-FW-IPS(config)#int gig0/3
ASA-FW-IPS(config-if)#nameif Inside
ASA-FW-IPS(config-if)#security-level 100
ASA-FW-IPS(config-if)#ip address 172.16.32.2 255.255.255.248
ASA-FW-IPS(config-if)#no shutdown
ASA-FW-IPS(config-if)#exit
```

## - Internal Router

```
Internal-Router>enable
Internal-Router#conf t
Internal-Router(config)#int fa0/0
Internal-Router(config-if)#ip address 172.16.32.1 255.255.255.248
Internal-Router(config-if)#no shutdown
Internal-Router(config-if)#exit
Internal-Router(config)#int fa0/1
Internal-Router(config-if)#ip address 10.234.100.1 255.255.255.0
Internal-Router(config-if)#no shutdown
Internal-Router(config-if)#exit
```

- Champaigne Gateway Router

```
Champaigne_GatewayRouter>enable
Champaigne_GatewayRouter#conf t
Champaigne_GatewayRouter(config)#int fa0/0
Champaigne_GatewayRouter(config-if)#ip address dhcp
Champaigne_GatewayRouter(config-if)#no shutdown
Champaigne_GatewayRouter(config-if)#exit
Champaigne_GatewayRouter(config)#int fa0/1
Champaigne_GatewayRouter(config-if)#ip address 80.0.1.2 255.255.255.248
Champaigne_GatewayRouter(config-if)#no shutdown
Champaigne_GatewayRouter(config-if)#exit
Champaigne_GatewayRouter(config)#
```

- Champaigne Palo Alto

Follow same procedure above to configure champaigne palo alto

## NETWORK SECURITY

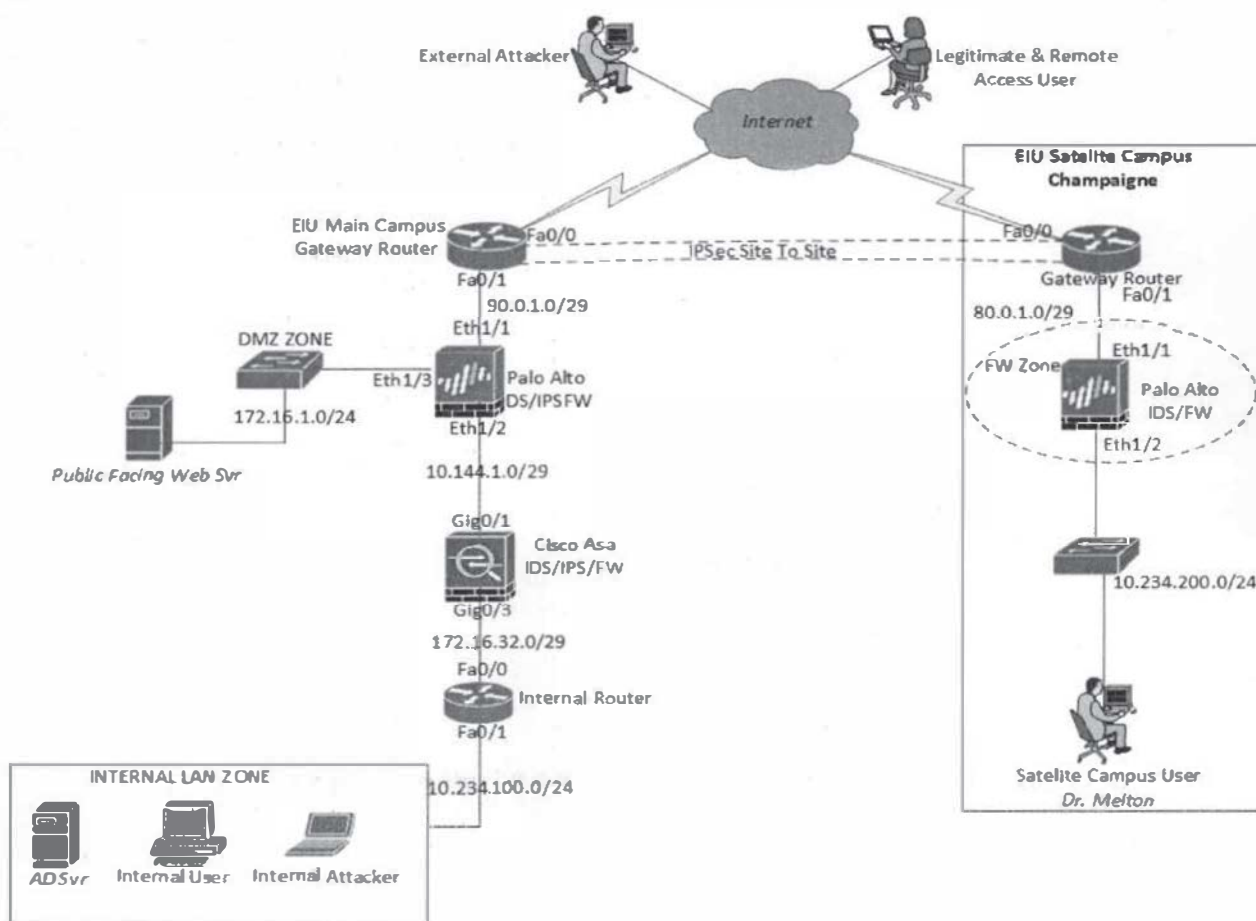
### LABORATORY II: NAT: ACCESSING THE INTERNET

**Lab Purpose:** The purpose of this lab exercise is to introduce students to NAT; Network Address Translation. NAT allow multiple private ip address users to access the internet with a single shared public ip address. We will also be introduce to static NAT, by statically NATting the private ip address of the web server to our public ip address can be able to access the webserver with the public ip address.

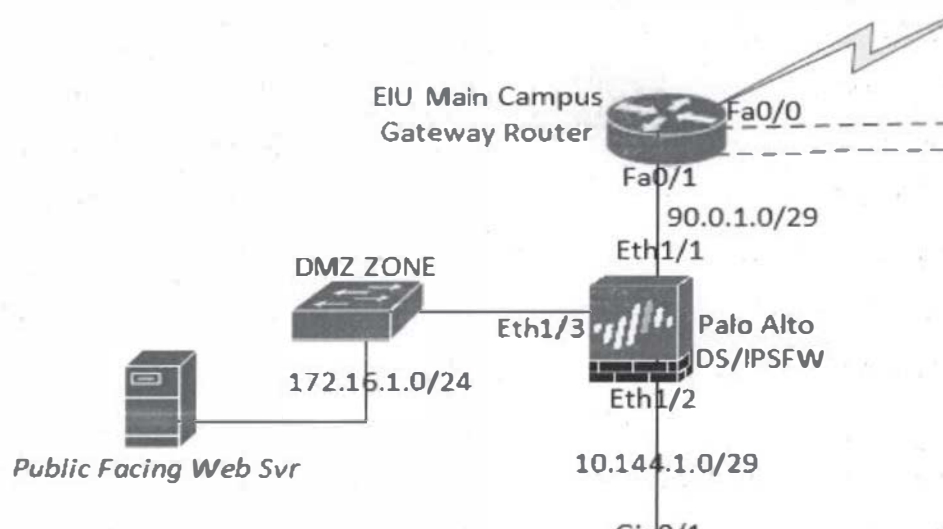
**Assumption:** It is assumed that students have some basic knowledge in networking.

**Task:**

The network topology below has been physically connected, configure NAT on the EIU Main campus gateway router so that internal lan zone can access the internet and users from the internet can access the web server using the public ip address of int fa0/0.







### Solution Guide

- EIU Main Campus Gateway Router
- Create Access-list for the permitted traffic

```
EIU_Main_Campus>enable
EIU_Main_Campus#Conf t
EIU_Main_Campus(config)# access-list 105 permit ip any any
```

The above access-list is permitting all traffic from the internal network to any network on the internet.

- Configure the NAT

```
EIU_Main_Campus(config-if)#int fa0/0
EIU_Main_Campus(config-if)#ip nat outside
EIU_Main_Campus(config-if)#exit
Boundary_Router(config)#int fa0/1
Boundary_Router(config-if)#ip nat inside
Boundary_Router(config-if)#exit
Boundary_Router(config)# ip nat inside source list 105 interface FastEthernet0/0
overload
```

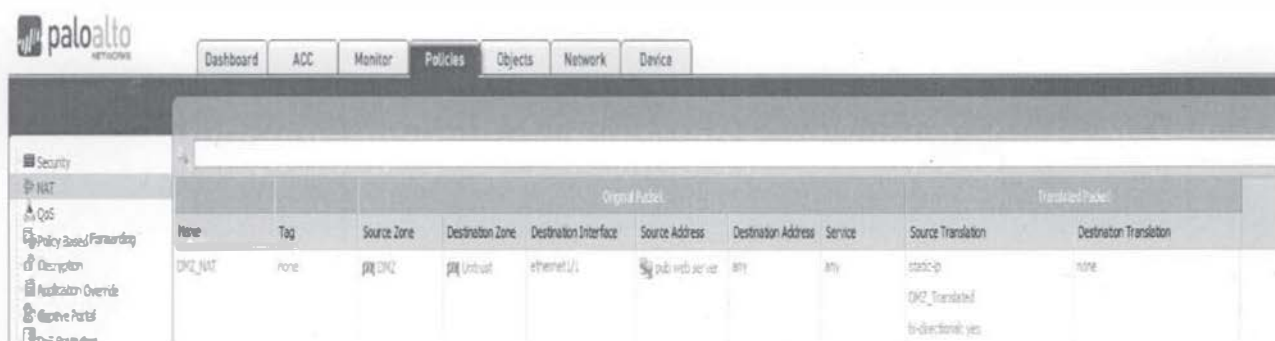
NAT Overloading or Port Address Translation (PAT) is a modified form of dynamic NAT where the number of inside local addresses is greater than the number of inside global addresses. Mostly, there is just a single inside global IP address providing Internet access to all inside hosts.

- Now configure Static NAT for internet users to be able to access the web server with EIU Main Gateway router public facing interface ip address.

```
Boundary_Router(config)# ip nat inside source static tcp 90.0.1.1 80 192.168.1.151 80
extendable
```

Here the router is configured to NAT to the Palo Alto Outside interface (90.0.1.1) which is then configured to do static NATting to the web server which is 172.16.1.2.

- Configure the static NAT on Palo Alto to the web server



Addresses	
<input type="text"/> <input type="button" value="→"/> <input type="button" value="✕"/>	
Name	Address
DMZ	172.16.1.0/24
DMZ_Transla...	90.0.1.1/32
LAN_Network	10.234.100.0/24
pub web ser...	172.16.1.2

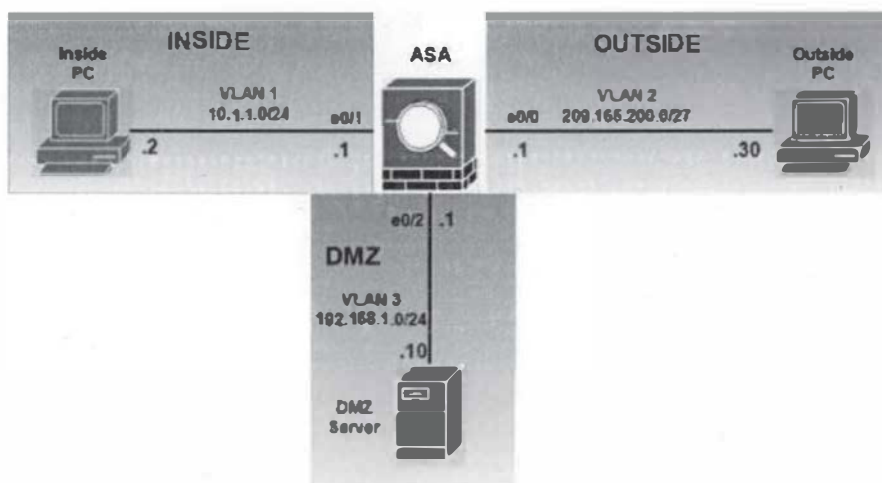
## ASA FIREWALL

### LAB 1: AUTO NAT AND MANUAL NAT

**Lab Purpose:** The purpose of this lab is to learn how to configure Network Address Translation in ASA firewall. As we have learnt in previous lab how to configure it in a cisco router, we are going to learn how it is configured in ASA firewall.

Configure the basic IP addressing for the CISCO ASA interfaces.

## Lab-1: Auto NAT and Manual NAT



- Connect the rollover console cable to the ASA console port (i.e. USB to Serial)
- Check the "Computer management" in your PC and then check "device manager" (PORT COM&LPT) and for the available serial port (i.e. COM 7" or other)
- Using PUTTY (Double click) in your desktop, click on serial and change the appropriate COM port in step a) , use 9600 bits/sec as default connection speed) , then click "open"
- Press enter and program the ASA as follows

```

Ciscoasa>enable (NO password , just press enter)
Ciscoasa#config t
Ciscoasa(config)#int gig0/1
Ciscoasa(config-if)#no shutdown
Ciscoasa(config-if)#nameif inside
Ciscoasa(config-if)#security-level 100
Ciscoasa(config-if)#ip address 10.1.1.1 255.255.255.0
Ciscoasa(config-if)#exit
Ciscoasa(config)#int gig0/0
Ciscoasa(config-if)#no shutdown
Ciscoasa(config-if)#nameif outside
Ciscoasa(config-if)#security-level 0
Ciscoasa(config-if)#ip address 209.165.200.1 255.255.255.224
  
```

```

Ciscoasa(config-if)#exit
Ciscoasa(config)#int gig0/2
Ciscoasa(config-if)#no shutdown
Ciscoasa(config-if)#nameif dmz
Ciscoasa(config-if)#security-level 50
Ciscoasa(config-if)#ip address 192.168.1.1 255.255.255.0

```

- e) By default the echo-reply ICMP is not allowed from a lower security to a higher security, enabling ICMP inspection in the policy-map global\_policy:

```

Ciscoasa(config)# policy-map global_policy
Ciscoasa(config-pmap)# class inspection_default
Ciscoasa(config-pmap-c)# inspect icmp

```

- f) Auto-NAT Configuration: The following procedure is one of the way to program NAT and is configure under object network

**Task1:** The DMZ server requires a static translation when routed to the outside interface. The translated ip address is 209.165.200.22:

```

Ciscoasa(config)# object network DMZ-SRV
Ciscoasa(config-network-object)# host 192.168.1.10
Ciscoasa(config-network-object)# nat (dmz, outside) static 209.165.200.22

```

- g) Access the public server from the DMZ computer/server (192.168.1.10) by typing <http://209.165.200.30> (Ask the GA to start the Web-server service on the public webserver [209.165.200.30] and on the DMZ webserver (192.168.1.10))
- h) check the translation after activity g) by typing (config) # show xlate

**From the DMZ Server connect to the Public Server:**



## OUTSIDE web Server

***WELCOME!***

**Task2:** The inside network requires PAT when routed to the outside interface, the hosts in the inside network share the same public IP address 209.165.200.20:

```

Ciscoasa(config)# object network INSIDE-NETWORK
Ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
Ciscoasa(config-network-object)# nat (inside, outside) dynamic 209.165.200.20

```

- i) Testing the translations: The show xlate command shown that the inside host with 10.1.1.2 is translated to 209.165.200.20

```
ciscoasa(config)# sh xlate
5 in use, 7 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.1.10 to outside:209.165.200.22
   flags s idle 0:01:15 timeout 0:00:00
TCP PAT from inside:10.1.1.2/49816 to outside:209.165.200.20/49816 flags ri idle 0:00:13 timeout 0:00:30
TCP PAT from inside:10.1.1.2/49815 to outside:209.165.200.20/49815 flags ri idle 0:00:13 timeout 0:00:30
TCP PAT from inside:10.1.1.2/49813 to outside:209.165.200.20/49813 flags ri idle 0:00:13 timeout 0:00:30
TCP PAT from inside:10.1.1.2/49811 to outside:209.165.200.20/49811 flags ri idle 0:00:13 timeout 0:00:30
ciscoasa(config)#
```

## ALTERNATIVE PROGRAMMING.

Manually programming NAT/PAT, is recommended when you have to include a policy at which at which it should translate when it's going to a particular destination.

To Begin; Clear previous configuration

```
Ciscoasa(config)# clear configure object
```

Manual Configuration

For The DMZ server, configure a translation that should be used only when the destination is the outside network is 209.165.200.0/27 using the translated Ip address 209.165.200.25:

```
Ciscoasa(config)# object network DMZ-SRV
```

```
Ciscoasa(config)# host 192.168.1.10
```

```
Ciscoasa(config)# exit
```

```
Ciscoasa(config)# object network OUTSIDE-NETWORK
```

```
Ciscoasa(config-network-object)# subnet 209.165.200.0 255.255.25.224
```

```
Ciscoasa(config-network-object)# exit
```

```
Ciscoasa(config)# object network DMZ-MANUAL-NAT
```

```
Ciscoasa(config-network-object)# host 209.165.200.25
```

```
Ciscoasa(config-network-object)# exit
```

```
Ciscoasa(config)# nat (dmz,outside) source static DMZ-SRV DMZ-MANUAL-NAT destination
static OUTSIDE-NETWORK OUTSIDE-NETWORK
```

Do show xlate

```
ciscoasa(config)# sh xlate
2 in use, 7 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from dmz:192.168.1.10 to outside:209.165.200.25
   flags sT idle 0:00:07 timeout 0:00:00
NAT from outside:209.165.200.0/27 to dmz:209.165.200.0/27
   flags sIT idle 0:00:07 timeout 0:00:00
ciscoasa(config)#
```

**Task3:** For inside clients, configure a translation that should be used when accessing the DMZ server on TCP port 8080, the inside hosts should use a single IP address 192.168.1.11 and the dmz server should see the port 80 instead of 8080:

```
Ciscoasa(config)# object network INSIDE-NETWORK
```

```
Ciscoasa(config)# subnet 10.1.1.0 255.255.255.0
```



```

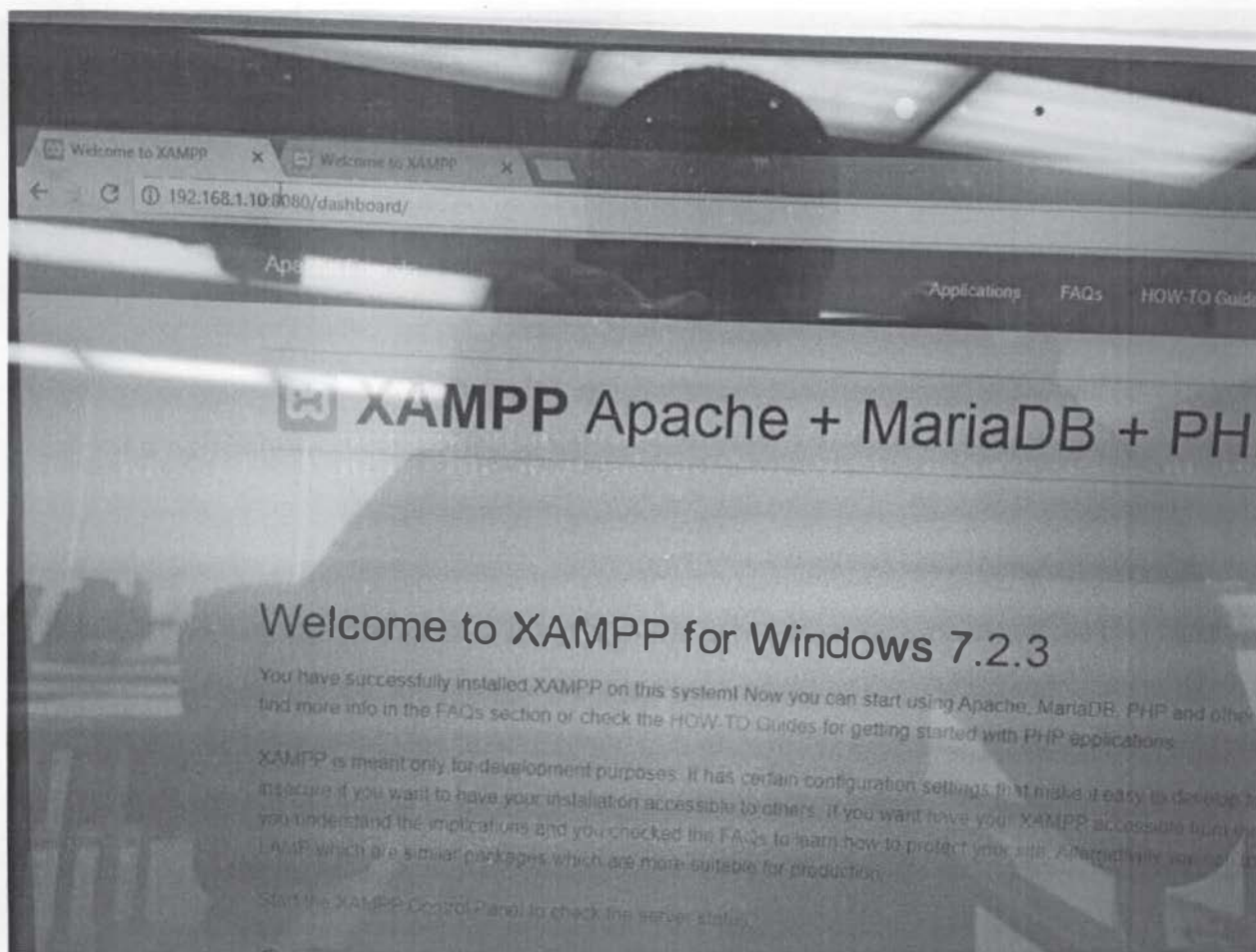
Ciscoasa(config)#exit
Ciscoasa(config)#object network DMZ_PAT
Ciscoasa(config-network-object)#host 192.168.1.11
Ciscoasa(config-network-object)#exit
Ciscoasa(config)#object service HTTP_80
Ciscoasa(config-service-object)#service tcp destination eq www
Ciscoasa(config-service-object)#exit
Ciscoasa(config)#object service HTTP_PROXY_PORT
Ciscoasa(config-service-object)#service tcp destination eq 8080
Ciscoasa(config)#nat (inside,DMZ) source dynamic INSIDE-NETWORK DMZ_PAT
destination static DMZ-SRV DMZ-SRV service HTTP_PROXY_PORT HTTP_80
From inside host, we can access the web server in dmz using http://192.168.1.10:8080

```

```

ciscoasa(config)# sh xlate
3 in use, 7 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
      s - static, T - twice, N - net-to-net
NAT from dmz:192.168.1.10 to outside:209.165.200.25
  flags sT idle 0:05:12 timeout 0:00:00
NAT from outside:209.165.200.0/27 to dmz:209.165.200.0/27
  flags sIT idle 0:05:12 timeout 0:00:00
TCP PAT from dmz:192.168.1.10 80-80 to inside:192.168.1.10 8080-8080
  flags srIT idle 0:01:11 timeout 0:00:00
ciscoasa(config)#

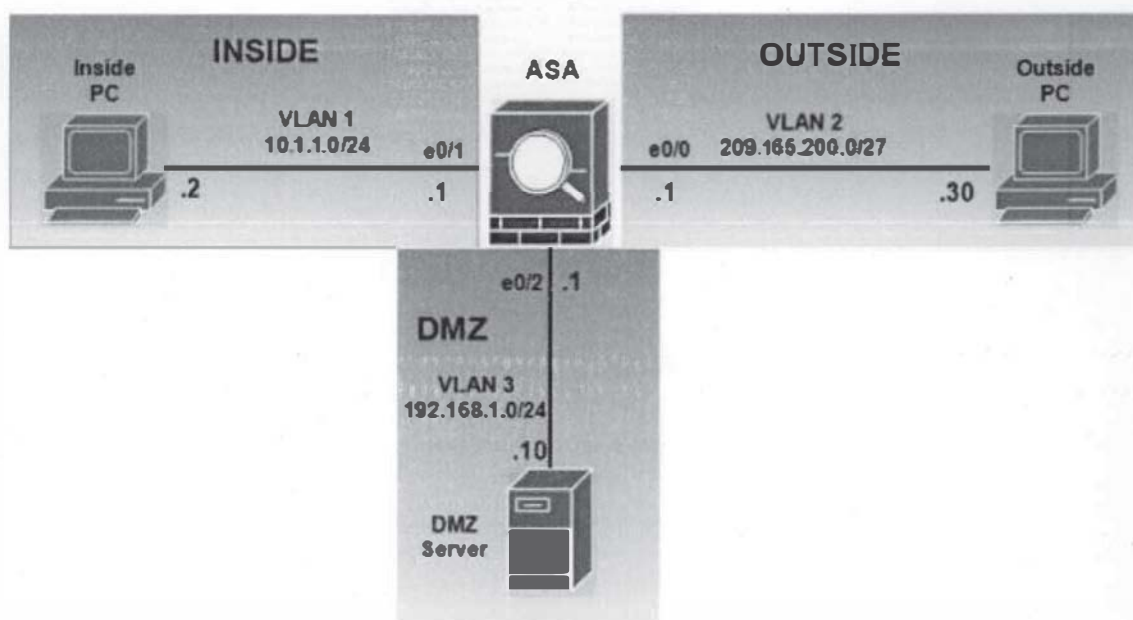
```





## LAB 2: HTTP INSPECTION

**Lab Purpose:** The purpose of this lab is to learn the default behavior of how an ASA firewall inspect http traffic and to configure it.



**Task 1:** By default ASA does not allow a traffic to traverse from a lower security level to a higher security level. We should configure an access list OUT-TO-DMZ that permits HTTP traffic from the outside server to the internal IP address of the DMZ server. Apply the access list to the ASA outside interface in the “IN” direction.

**Solution:**

```
Ciscoasa>enable
```

```
Ciscoasa#conf t
```

To Begin with, clear all previous configurations

```
Ciscoasa(config)#clear configure nat
```

```
Ciscoasa(config)#clear configure object
```

Then Start Configuration

```
Ciscoasa(config)#object network DMZ-SERVER-PRIV
```

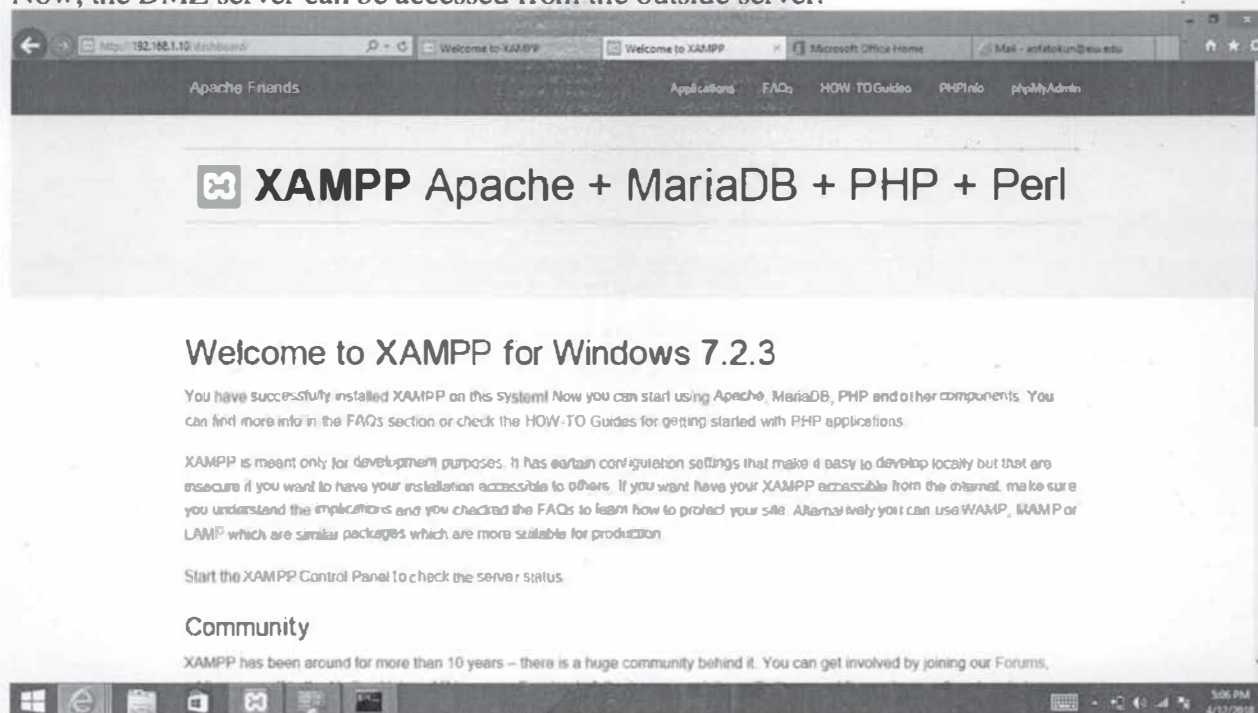
```
Ciscoasa(config)#host 192.168.1.10
```

```
Ciscoasa(config)#exit
```

```
Ciscoasa(config)#access-list OUT-TO-DMZ extended permit tcp host 209.165.200.30 object DMZ-SERVER-PRIV eq www
```

```
Ciscoasa(config)#access-group OUT-TO-DMZ in interface outside
```

Now, the DMZ server can be accessed from the outside server.



Another method that can be used to allow http traffic from lower security level to higher security is when the traffic initially originated from a higher security level, the return traffic of such traffic will be allow in from a lower security level to a higher security level.

**Task 2:** Without using access-list, configure the ASA to allow inbound return traffic of http from a lower security level to a higher security level. In other words we will inspect if the traffic has been originated in the inside or not and then allow it if originated from the inside.

**Solution**

We are going to make use of modular policy framework (MPF) and by default the ASA does not inspect http traffic so we need to enable it.

Modular Policy Framework (MPF) configuration defines set of rules for applying firewall features, such as traffic inspection, QoS etc. to the traffic transiting the firewall.

```
Ciscoasa>enable
Ciscoasa#config t
Ciscoasa(config)#policy-map global_policy
Ciscoasa(config-pmap)#class inspection_default
Ciscoasa(config-pmap-c)#inspect http
Ciscoasa(config-pmap-c)#exit
Ciscoasa(config-pmap)#exit
Ciscoasa(config)#
```

What we have done is to inspect all http traffic that originate from inside, this will create a session table and all return traffic of that traffic will allow in from lower security level to a higher security level.

Task 3: We are also going to use http inspection to drop all bad http traffic from coming into the network. Bad traffic in this case are traffic that uses http port number other than the web traffic, for example telnet traffic trying to use port 80 instead of port 23.

Configure HTTP inspection between any host from outside and the dmz server to verify conformance to the http protocol.

Solution:

- Create a NAT to allow the DMZ server to be accessed from the outside network
- Create an http inspection policy-map named HTTP-Policy
- Enable the HTTP protocol verification to drop and log all HTTP sessions that do not conform to the standard protocol specifications.

Ciscoasa>enable

Ciscoasa#config t

To start with, clear all previous object configuration and nat configuration.

Ciscoasa(config)#clear configure object

Ciscoasa(config)#clear configure nat

Now start the configuration

Ciscoasa(config)#object network DMZ-SRV1

Ciscoasa(config)#host 192.168.1.10

Ciscoasa(config)#nat (dmz,outside) static 209.165.200.22

Ciscoasa(config)#exit

Ciscoasa(config)#policy-map type inspect http HTTP-POLICY

Ciscoasa(config-pmap)#parameters

Ciscoasa(config-pmap-p)#protocol-violation action drop-connection log

- Now, create a new traffic class inside the global-policy with the following parameters

Traffic class name: WEB-PROTECTION

Traffic Matching: From the ANY to the DMZ Server

Apply the configured HTTP-Policy HTTP inspection policy-map

Ciscoasa(config)#object network DMZ-SERVER-PRIV

Ciscoasa(cisco)#host 192.168.1.10

Ciscoasa(config)#exit

Ciscoasa(config)#access-list GLOBAL-DMZ extended permit tcp any object DMZ-SERVER-PRIV eq www

Ciscoasa(config)#class-map WEB-PROTECTION

Ciscoasa(config)#match access-list GLOBAL-DMZ

Ciscoasa(config)#policy-map global\_policy

Ciscoasa(config-pmap)#class WEB-PROTECTION

Ciscoasa(config-pmap-c)#inspect http HTTP-POLICY

In order to check the policy type

ciscoasa# sh service-policy global

The following figure should be seen

```

ciscoasa# show service-policy global

Global policy:
Service-policy: global_policy
Class-map: inspection_default
Inspect: dns preset_dns_map, packet 0, drop 0, reset-drop 0
Inspect: ftp, packet 0, drop 0, reset-drop 0
Inspect: h323 h225 _default_h323_map, packet 0, drop 0, reset-drop 0
Inspect: tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: h323 ras _default_h323_map, packet 0, drop 0, reset-drop 0
Inspect: rsh, packet 0, drop 0, reset-drop 0
Inspect: rtsp, packet 0, drop 0, reset-drop 0
Inspect: tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: esmtp _default_esmtp_map, packet 0, drop 0, reset-drop 0
Inspect: sqlnet, packet 0, drop 0, reset-drop 0
Inspect: skinny , packet 0, drop 0, reset-drop 0
Inspect: tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: sunrpc, packet 0, drop 0, reset-drop 0
Inspect: tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: xdmp, packet 0, drop 0, reset-drop 0
Inspect: sip , packet 0, drop 0, reset-drop 0
Inspect: tcp-proxy: bytes in buffer 0, bytes dropped 0
Inspect: netbios, packet 16, drop 0, reset-drop 0
Inspect: tftp, packet 0, drop 0, reset-drop 0
Inspect: ip-options _default_ip_options_map, packet 0, drop 0, reset-drop 0
Inspect: icmp, packet 29, drop 0, reset-drop 0
Class-map: WEB-PROTECTION
Inspect: http HTTP-POLICY, packet 0, drop 0, reset-drop 0
ciscoasa#

```

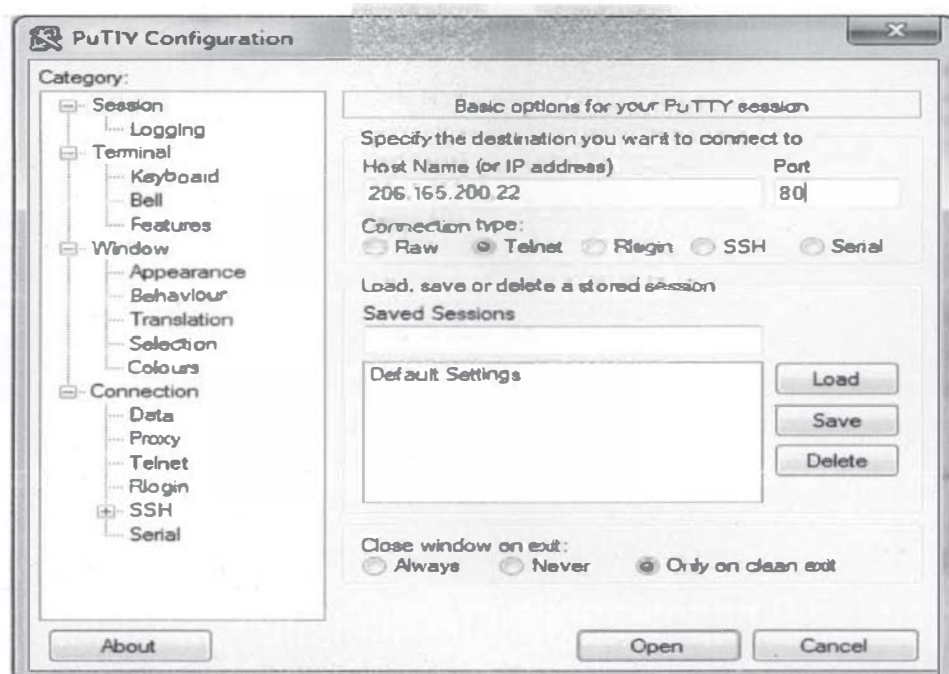
### Testing and Verification

From the outside server access the web page of the DMZ server through a web browser, we can see below that the attempt is successful: Based on the NAT configuration, we can access the DMZ server from outside network using 209.165.200.22 which will be translated to 192.168.1.10.



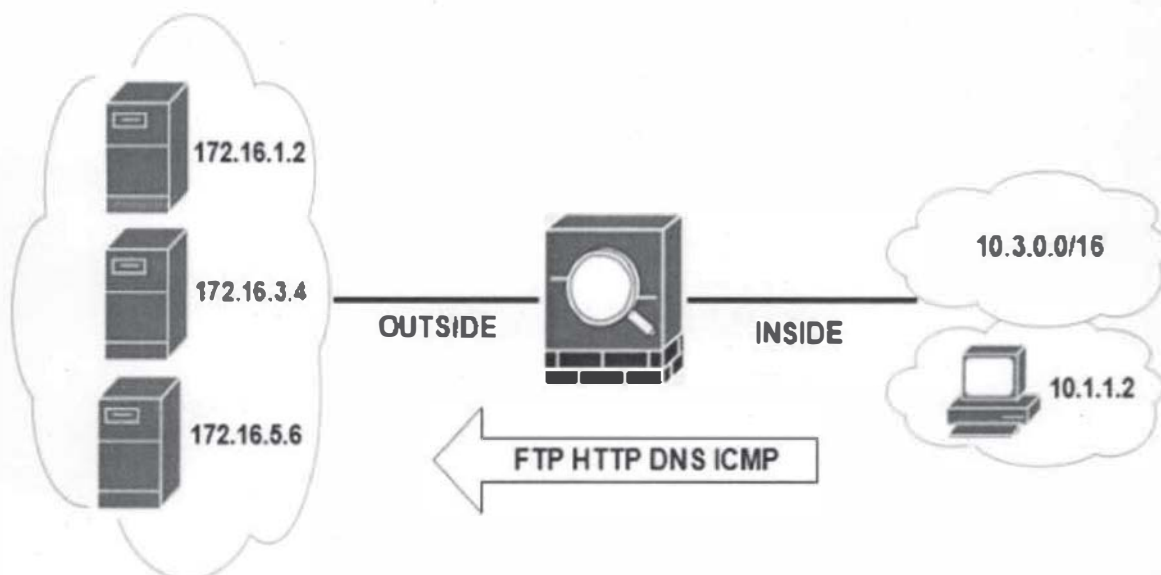
Now open putty in the outside server and access the DMZ server 209.165.200.22 with telnet using a port 80: This will be dropped because it's a bad http traffic, we are trying to telnet using http protocol port no:80





## LAB : ACCESS-LIST ACL USING NETWORK OBJECT

**Lab Purpose:** The purpose of this lab is to learn how to use network object to group access-list entries for easy configuration for traffic filtering.



### Notes:

A set of interface access rules can cause the Cisco ASA to permit or deny a designated host to access another particular host with a specific network application (service). When there is only one client, one host and one service, you need only a minimum number of lines in an interface rule set. However, as the number of clients, servers, and services increases, the number of rules that you need for each individual access type can increase and become unmanageable.

A better approach is to introduce object grouping. This solution allows you to arbitrarily group hosts, resources, or services that share the same policy, which optimizes the access rules.

In our scenario above, the ASA control traffic between an internal enterprise network that is connected over the inside interface and an external network that is connected over the outside interface.

The internal subnet 10.3.0.0/16 and the internal client 10.1.1.2 should both have permanent HTTP, FTP, DNS and ICMP access to a group of external servers (172.16.1.2, 172.16.3.4 and 172.16.5.6)

**Task 1:** Create a network object for the network 10.3.0.0/16 and the host 10.1.1.2:

### Solution

```
Ciscoasa>enable
```

```
Ciscoasa#config t
```

```
Ciscoasa(config)#object network NETWORK-CLIENT
```

```
Ciscoasa(config-obj-network)#subnet 10.3.0.0 255.255.255.0
```



```
Ciscoasa(config-obj-network)#exit
Ciscoasa(config)#object network PC-CLIENT
Ciscoasa(config-obj-network)#host 10.1.1.2
```

Task 2: Create a network object for the external servers:

```
Ciscoasa(config-obj-network)#exit
Ciscoasa(config)#object network SERVERS-A
Ciscoasa(config-obj-network)#host 172.16.1.2
Ciscoasa(config-obj-network)#exit
Ciscoasa(config)#object network SERVERS-B
Ciscoasa(config-obj-network)#host 172.16.3.4
Ciscoasa(config-obj-network)#exit
Ciscoasa(config)#object network SERVERS-C
Ciscoasa(config-obj-network)#host 172.16.5.6
Ciscoasa(config-obj-network)#exit
```

Task 3: Creates a network object group for the clients (Grouping the clients)

```
Ciscoasa(config)#object-group network INTERNAL
Ciscoasa(config)#network-object object NETWORK-CLIENT
Ciscoasa(config)#network-object object PC-CLIENT
```

Task 4: Create a network object group for the servers:

```
Ciscoasa(config)#object-group network EXTERNAL-SERVERS
Ciscoasa(config)#network-object object SERVERS-A
Ciscoasa(config)#network-object object SERVERS-B
Ciscoasa(config)#network-object object SERVERS-C
```

Task 5: Creates a service object group:

```
Ciscoasa(config)#object-group service CLIENT-SERVICES
Ciscoasa(config)#service-object icmp echo
Ciscoasa(config)#service-object tcp destination eq ftp
Ciscoasa(config)#service-object tcp destination eq http
Ciscoasa(config)#service-object udp destination eq domain
Ciscoasa(config)#service-object tcp destination eq domain
```

Task 6: Configure an ACL that uses network and service object groups:

```
Ciscoasa(config)#access-list INSIDE-ACL extended permit object-group CLIENT-SERVICES
object-group INTERNAL Object-group EXTERNAL-SERVERS
```

Task 7: Apply the ACL inbound of the inside interface:

```
Ciscoasa(config)#int gig0/1
Ciscoasa(config-if)#access-group INSIDE-ACL in interface inside
```

Task 8: Test the policy by typing Ciscoasa(config) #sh run object-group

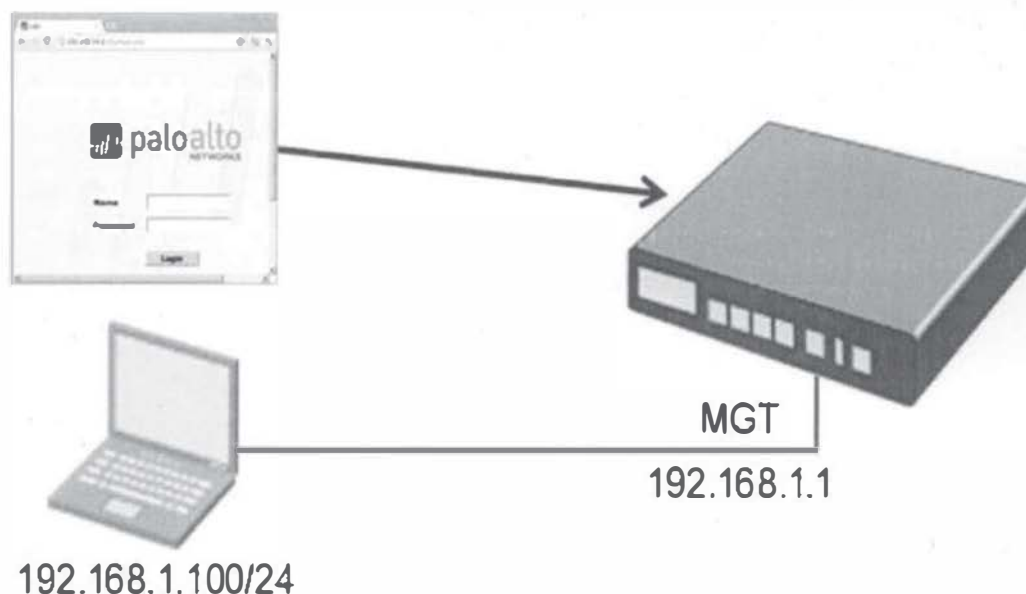
```
ciscoasa# show run object-group
object-group network INTERNAL
  network-object object NETWORK-CLIENT
  network-object object PC-CLIENT
object-group network EXTERNAL-SERVERS
  network-object object SERVER-A
  network-object object SERVER-B
  network-object object SERVER-C
object-group service CLIENT-SERVICES
  service-object icmp echo
  service-object tcp destination eq ftp
  service-object tcp destination eq www
  service-object udp destination eq domain
ciscoasa#
```

## PALO ALTO FIREWALL LAB PRACTICES

### LAB 1: PALO ALTO INITIAL WEB ADMINISTRATION AND MANAGEMENT

In this lab you will:

- Connect to the firewall through the MGT interface
- Create new administrator roles and accounts on the firewall

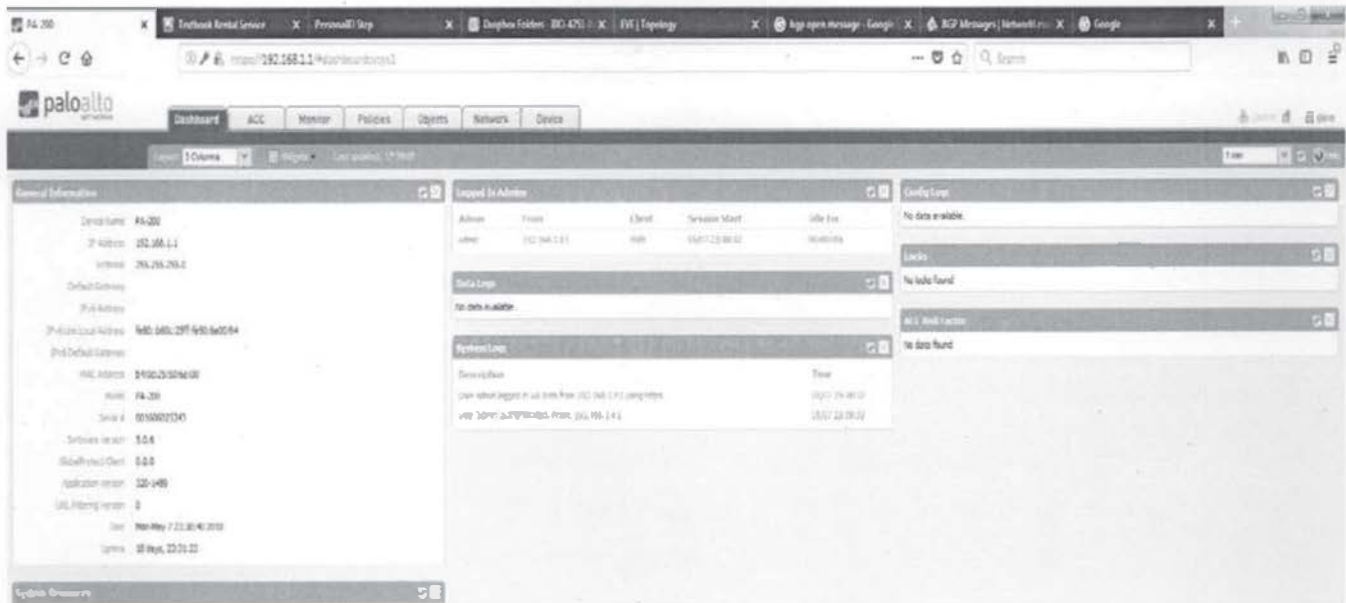


**Task 1:** The Palo Alto firewall is recently acquired firewall, the management interface typically comes with a default IP address 192.168.1.1/24. Configure your computer in the IP address range of the MGT port of the device to have access to the web interface with a default username/password of admin/admin.

**Solution**

- Configure the physical Ethernet interface of your laptop with an IP address on the same subnet as the MGT port of your firewall. (i.e. TCP/IP settings of the NIC card)
- If your firewall is at default configuration, the IP address of the MGT port is 192.168.1.1/24. Give your laptop Ethernet port an address of 192.168.1.100/24.
- If your firewall is not at default configuration, give your laptop an IP address on the same subnet as the MGT port IP address.
- Connect an Ethernet cable between your laptop Ethernet port and the MGT port of your firewall.
- Open a command prompt on your laptop and verify you can ping the MGT port IP address.
- Disable any other active interfaces on your laptop, including the wireless interface, so the Ethernet port connected to the firewall is your only active port.

- Access the management IP address of the firewall on a web browser <https://192.168.1.1> (or the default IP address assigned to the Firewall)
- Type in the username/password as admin/admin. A warning about the default admin credentials appears.
- Click OK to dismiss the warning for now. The PAN firewall GUI appears.



**Task 2:** Change the password of the *admin* account to EIULAB to disable the warnings about using default credentials.

### Solution

- On the WEBUI of the firewall, Click Device> Administrators
- Click admin in the list of users. Change the password from admin to EIULAB. Click OK to close the configuration window. (leave the SSH PKA uncheck)

**Task 3:** Create a role for an assistant administrator which will allow access to all firewall functionality through the WEBUI except Monitor, Network, Privacy, and Device. Create an account using this role.

**Solution**

- Click Device> Admin Roles.(in the left pane)
- Click Add in the lower left of the panel and create a new admin role:
- Type *Policy Admins* in the name window

Web UI tab categories	Click the following major categories to disable them: <ul style="list-style-type: none"> <li>• Monitor</li> <li>• Network</li> <li>• Device</li> <li>• Privacy</li> </ul> The remaining major categories should remain enabled.
-----------------------	---

- Click OK to continue.

**Task 4:** Create a general account

- Click Device> Administrators.
- Click Add in the lower left corner of the panel. Configure a new administrator account:

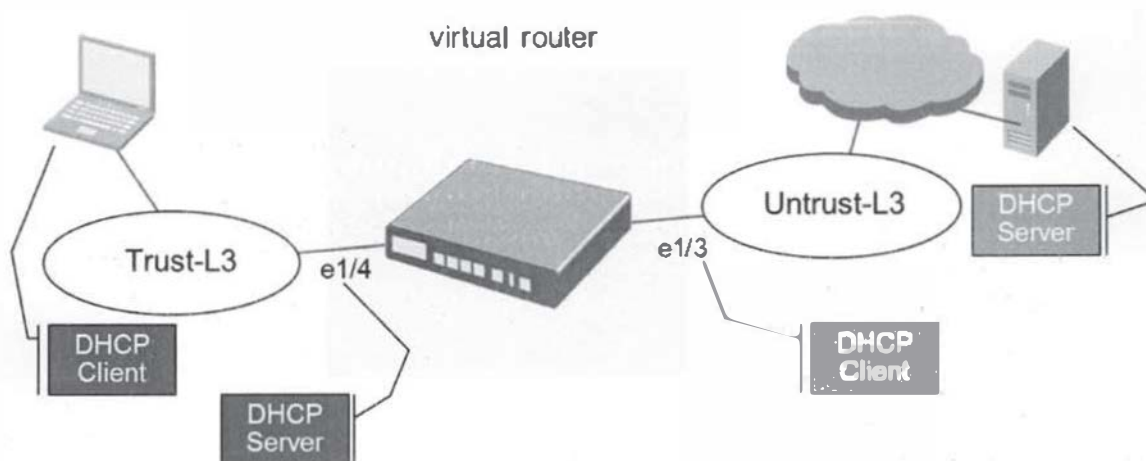
Name field	Type ip-admin
Password/Confirm Password	Type paloalto
Role	Select Role Based
Profile	Select Policy Admin (scroll down menu)
SSH	Leave it uncheck

- Click OK
- To save your configuration, click the Commit link at the top-right of the WEBUI. Click OK to the commit pop- up window and wait until the commit process completes, then click Close.

## LAB 2: Layer 3 Configuration

In this lab you will:

- Create Interface Management Profiles
- Configure Ethernet interfaces with Layer 3 information
- Configure DHCP



### Task 1: Create new Security Zones

Create two zones, Untrust-L3 and Trust-L3, interface e1/3 should be assigned to the Untrust-L3 zone, while interface e1/4 should be assigned to the Trust-L3 zone.

1. Go to the WEBUI and click the Network tab > Zones (in the left pane)
2. Click Add and create the Untrust-L3 zone:

Name	type Untrust-L3
Type	Verify that Layer 3 is selected

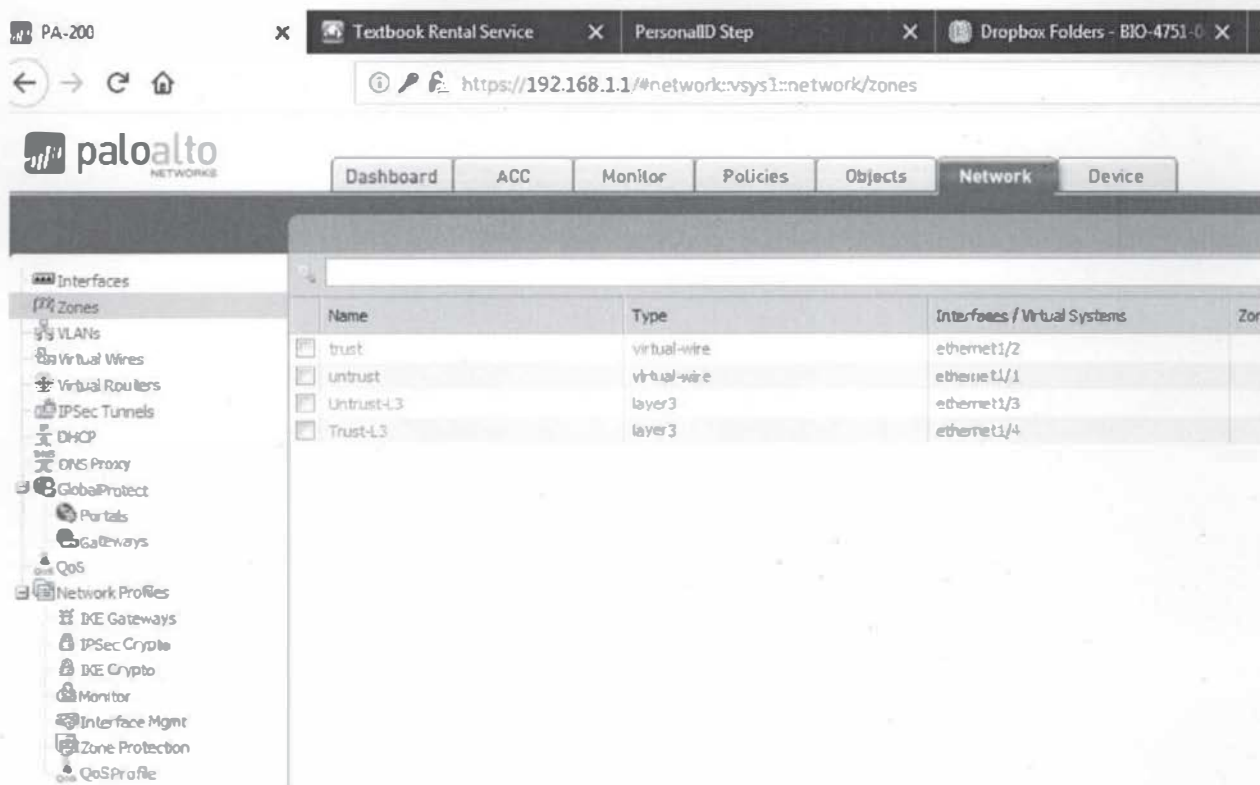
Click OK to close the zone creation window.

3. Click Add and create the Trust-L3 zone:

Name	type Trust-L3
Type	Verify that Layer 3 is selected

Click OK to close the zone creation window.





### Task 2: Create Interface Management Profiles

Configure the interface in Untrust-L3 to be able to respond to pings and the interface in Trust-L3 to be able to provide all management services.

The Interface in the Untrust zone should be a DHCP client, while interface in the Trust zone should have a static IP address 192.168.2.1/24

#### Solution

- Click Network > Network Profiles > Interface Mgmt
- Click Add and create an interface management profile as follows:

Name column	Type allow_all
Permitted Services	Check all boxes
Permitted IP Addresses	Do not add any addresses

Click OK to close the Interface Management Profile

- Click Add and create another interface management profile:

Interface Type	Select from draw down menu Layer 3
Config tab	
Virtual Router	Keep default (none)
Security Zone	Select Untrust-L3
IPv4 tab	
DHCP Client	Select DHCP Client
Advanced tab > Other Info tab	
Management Profile	Select allow_ping
Name column	type allow_ping
Permitted Services	check only the Ping check box
Permitted IP Addresses	Do not add any addresses

Click OK to close the interface management profile creation window.

- Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

### Task 3: Configure Ethernet interfaces with Layer 3 info

- Click the Network tab > Interfaces > Ethernet tab
- Click the interface name ethernet1/3. Configure the interface:

*Note: Do check any other box if not instructed to do so*

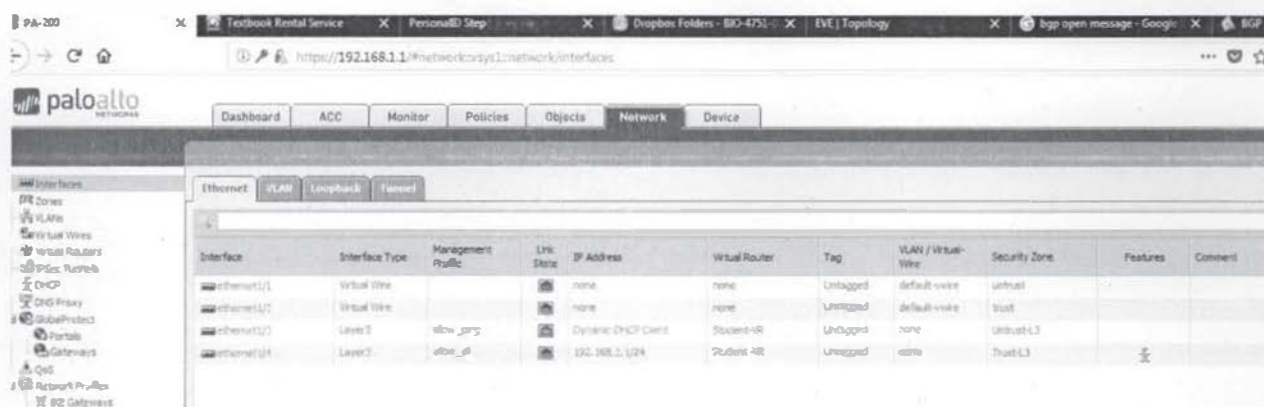
Click OK to close the interface configuration window.

- Click the interface name ethernet1/4. Configure the interface:

Interface Type	Select Layer 3
Config tab	
Virtual Router	Keep default (none)
Security Zone	Select Trust-L3
IPv4 tab	
Type	Keep default (Static)
IP	Click Add then type 192.168.2.1/24

Advanced > Other Info	
Management Profile	Select allow_all

Click OK to close the interface configuration window.  
 You should see both interfaces on green as shown in the next figure, if the  
 interfaces are not  
 Green call your instructor



#### Task 4: Configure DHCP

The Trust-L3 zone will be where the internal clients connect to the firewall and so the interface in Trust-L3 will provide DHCP addresses to these internal clients. The DHCP server you configure in the Trust-L3 zone will inherit DNS settings from the external facing interface.

#### Solution

11. Click the Network tab > DHCP > DHCP Server.

12. Click Add to define a new DHCP Server:

Interface Name	Select ethernet1/4
Inheritance Source	Select ethernet1/3
Gateway	Enter 192.168.2.1
Primary DNS	Select inherited
IP Pools	Click Add then enter 192.168.2.50-192.168.2.60

Click OK to close the DHCP Server configuration window.

#### Testing the DHCP Server configuration

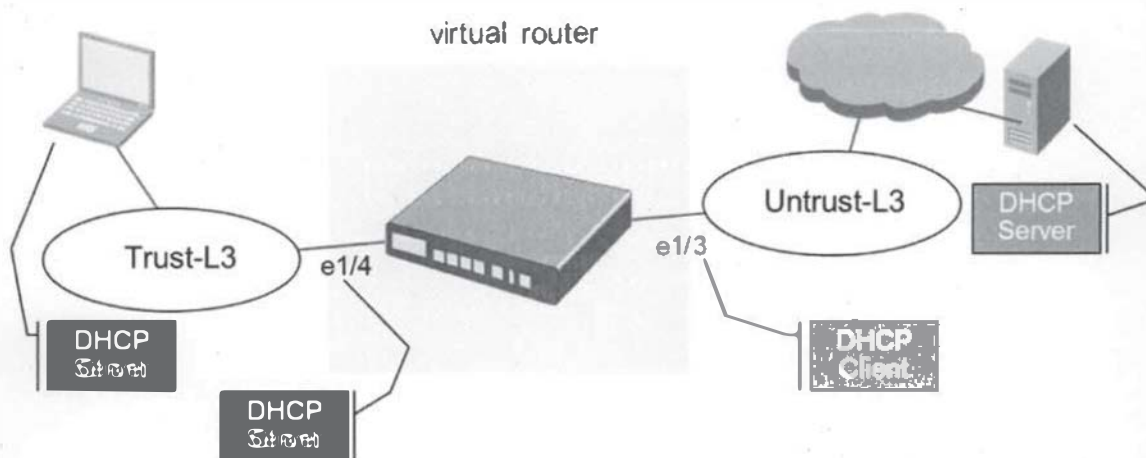
13. Connect a laptop to e1/4 and make sure the laptop NIC setting is set to DHCP.

Please note, your laptop will not get an IP address until you complete Laboratory

### LAB 3: Virtual Router and NAT Configuration

In this lab you will:

- Create a Virtual Router
- Create Source NAT policy
- Create a pair of simple Security Policies



#### Task 1: Create a Virtual Router

Configure a virtual router on the firewall so that the internal and external interfaces on the firewall must route traffic through the external-facing interface by default

**Solution**

1. Click the Network tab > Virtual Routers (in the left pane)
2. Click Add to define a new virtual router:

General tab	
Name	type Student-VR

Interfaces pane	<p>Click Add then select ethernet I/3</p> <p>Click Add again and select ethernet I/4</p>
-----------------	--

*Remember: Do not select or type in boxes you have not instructed to do so*  
Click OK to close the virtual router configuration window.

- Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

### Task 2: Create a Source NAT policy

Configure a NAT policy so that all traffic originating in the Trust-L3 zone appears to come from the external-facing address of the firewall.

#### Solution

- Click the Policies tab > NAT (on the left pane)
- Click Add to define a new source NAT policy:

General tab	
Name	Type Student_Source_NAT
Original Packet tab	
Source Zone pane	Click Add and select Trust-L3
Destination Zone	Select Untrust-L3
Destination Interface	Select ethernet I/3
Translated Packet > Source Address Translation tab	
Translation Type	Select Dynamic IP and Port
Address Type	Select Interface Address
Interface	Select ethernet I/3

Click OK to close the NAT policy configuration window.





6. Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

You will still not be able to access the Internet from your PC. The final task will be to create the Security Policies to allow traffic to flow from the Trust-L3 to the Untrust-L3 zone

### Task 3: Create Security Policies

7. Click the Policies Tab > Security (left pane)

8. Delete any configure rule (Highlight the policy (i.e. click) and then click "delete"

9. Click Add to define a new security policy

Give it a Name: Internet-Security-Rule

Source > Click Add > Trust-L3

Destination > Click Add > Untrust-L3

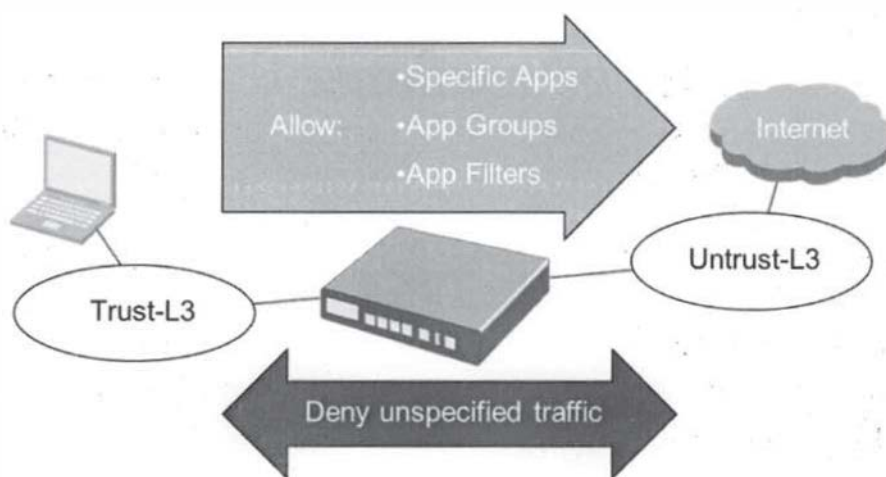
Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

Task 5: Check that you are able to connect to the internet from your computer or the LAPTOP connect to the Palo Alto firewall

### LAB 4: APP-ID

In this lab you will:

- Create a security policy to allow basic internet connectivity and log dropped traffic
- Enable Application Block pages
- Create Application Filters and Application Groups



#### Task 1: Create the Allow All Out Policy

At this point, the firewall is configured with the basics (i.e. IP addresses in interfaces) but is not able to pass traffic. Security policies must be defined before traffic will flow between zones. Configure a Policy to allow all outbound traffic, and to block and log any incoming traffic. This will allow employees to surf the Internet, and will allow the firewall to log which applications they have used.

**Solution**

1. Go to the WebUI and click Policies > Security (Top of left pane)
2. Delete any existing security policy.(click on the policy and then click delete at the bottom)
3. Click Add to define a security policy:

General tab	
Name	Type Allow_All_Out
Source tab	

Source Zone	Click Add and select Trust-L3
Source Address	Select Any
Destination tab	
Destination Zone	Click Add and select Untrust-L3
Destination Address	Select Any
Application tab	
Applications	Select Any
Service/URL Category tab	
Service	Select Any from the pull-down
Actions tab	
Action Setting	Select Allow
Log Setting	Select Log at Session End

4. Click OK to close the security policy configuration window.

#### Create a Deny and Log Inbound Policy

5. Click Add to define the Deny In bound security policy:

General tab	
Name	Type Deny and Log Inbound
Source tab	
Source Zone	Click Add and select Untrust-L3
Source Address	Select Any
Destination tab	
Destination Zone	Click Add and select Trust -L3
Destination Address	Select Any
Application tab	
Applications	Check the Any box
Service/URL Category tab	
Service	Select Any from the pull-down
Actions tab	
Action Setting	Select Deny
Log Setting	Select Log at Session End

6. Click OK to close the security policy configuration window.

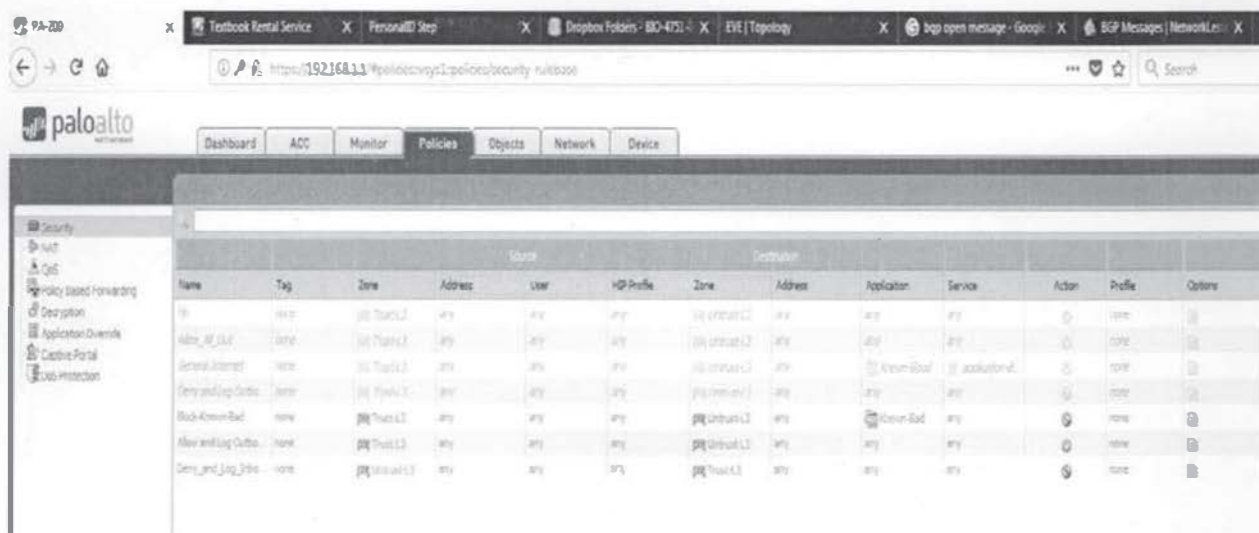
7. Make sure that the Allow All Out is above the Deny and Log Inbound policy in the list of Security

Policies.

If the Allow All out policy is not above the Deny and Log Inbound policy

Click to Highlight the policy, then click from the drop down menu, select Move and from there be sure to move the policy above or below

8. Before testing be sure the configuration looks like the following figure



Test the configuration

8. Test internet connectivity by browsing websites from your laptop. You should be able to surf the Web on http and https sites.

9. Connect to the site *facebook.com*

10. Connect to the site *box.net*

11. Go to Monitor > Logs > Traffic to see a record of your Internet browsing. Especially notice the Application column.

### Task 2: Create an Application Group

Create a *General Internet* policy to restrict users to a set of commonly used applications (dns, fileserve, flash, ftp, paloalto-updates, ping, web-browsing, ssl). The applications should only be permitted on application default ports. All other traffic (inbound and outbound) should be blocked and logged. Configure the firewall to notify users when blocked applications are used so that the help desk does not get called for “connection issues” that are actually blocked applications.

#### Solution

1. Click Objects > Application Groups.(on the left pane)
2. Click Add to define the *Known-Good* application group:

Name	Type Known-Good
Applications	Click Add and select each of the following: <ul style="list-style-type: none"> <li>• dns</li> <li>• fileserve</li> <li>• flash</li> <li>• ftp</li> <li>• paloalto-updates</li> </ul>

Click OK to close the application group configuration window.  
In order to Disable the Allow All Out Policy go to Policies > Security

3. Select the Allow All Out Policy and click Disable.

#### Create the General Internet Policy

4. Go to the WEBUI and click Policies > Security.
5. Click Add to define a security policy:

General tab	
Name	Type General Internet
Source tab	
Source Zone	Click Add and select Trust-L3
Source Address	Select Any
Destination tab	
Destination Zone	Click Add and select Untrust-L3



Destination Address	Select Any
<b>Application tab</b>	
Applications	Click Add and select the Known-Good Application
<b>Service/URL Category tab</b>	
Service	Select application-default from the pull-down
<b>Actions tab</b>	
Action Setting	Select Allow
Log Setting	Select Log at Session End

Click OK to close the security policy configuration window.

### Create Policies to Deny and Log All Outbound Traffic

6. Click Policies > Security.

7. Click Add to define the Deny and Log Outbound security policy:

<b>General tab</b>	
Name	Type Deny and Log Outbound
<b>Source tab</b>	
Source Zone	Click Add and select Trust-L3
Source Address	Select Any
<b>Destination tab</b>	
Destination Zone	Click Add and select Untrust-L3
Destination Address	Select Any
<b>Application tab</b>	
Applications	Check the Any box
<b>Service/URL Category tab</b>	
Service	Select any from the pull-down
<b>Actions tab</b>	
Action Setting	Select Deny
Log Setting	Select Log at Session End

Click OK to close the security policy configuration window.

8. Rearrange the Security Policies in the following order:

Click to Highlight the policy, then click from the drop down menu, select Move and from there be sure to move the policy above or below

a. General Internet



b. Deny and

Log

Outbound c.

Deny and

Log Inbound

Make sure any other Security Policies are disabled.

9. Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

#### Verify Internet Connectivity and Application Blocking

10. Test internet connectivity by browsing websites from your laptop. Does web surfing over ports 80 and

443 work? You may notice some difficulty reaching sites that you were able to reach before you implemented a stricter Security Policy.

11. Attempt to browse to Facebook. The browser should not be able to display the site.
12. Use a browser to connect to the site <http://www.box.net>. The browser should not be able to get to the display site.
13. Go to Monitor > Logs > Traffic to review the traffic logs to determine why this site is not reachable.

You can see that the *boxnet-base* and *facebook-base* applications are not allowed by the configured policies.

14. Attempt to reach the site <http://www.box.net> using the proxy site <http://www.avoidr.com>. The site fails to load.
15. Check the traffic logs again and you will find that the application *phproxy* has been blocked. This is why the *avoidr* site failed.

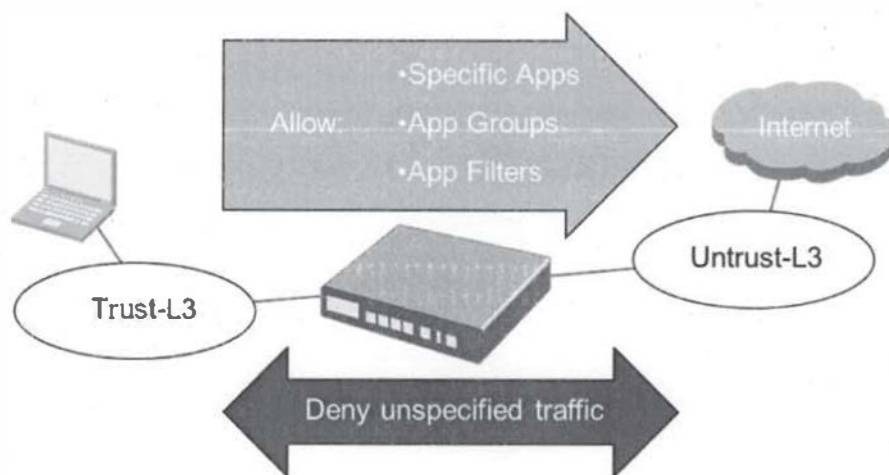
### Enable the Application Block Page

16. Return to the WEBUI and click Device > Response Pages.
17. Find the *Application Block Page* line and click Disabled.
18. Check the *Enable Application Block Page* box, and then click OK.
19. Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.
20. Open a browser window and go to <http://www.facebook.com>. This time you see an Application Block Page explaining why the site was blocked.

## LAB 5: APP-ID LAB II

In this lab you will: (this will enhance and continue the work of Lab 4)

- Create a security policy to allow basic internet connectivity and log dropped traffic
- Create Application Filters and Application Groups



Task I: The results from Lab 4 tasks testing, resulted in the following discoveries:

The logs from task 1 show heavy use of a variety of internet proxies and web-based file sharing services by users. Create a Deny list explicitly preventing the use of these applications.

The rules blocking all unmatched traffic were too restrictive for your environment. The testing, denied access to numerous vital applications, causing a surge in support calls. Any traffic which does not match the Deny list should be allowed but logged for future policy decision.

The following table shows a summary of the task we will accomplish in this lab

Application Filter names	Proxies
	Web-Based-File-Sharing

Security Policy names	Block-Known-Bad  Allow and Log Outbound
Setting for Proxies application filter	Subcategory: Proxies
Settings for Web-Based-File-Sharing application filter	Subcategory: file-sharing  Technology: browser-based
Members of the Known-Bad application group	Proxies  Web-Based-File-Sharing

### Solution:

#### Disable previous Security Policies

1. Click the Deny and Log Outbound rule and click the Disable button
2. Click the General Internet rule and click Disable button.

#### Create Application Filters and Groups

3. Go to the WEBUI and click Objects > Application Filters.
4. Click Add to define the Proxies application filter:

Name	Type Proxies
Subcategory column	Select proxy

Click OK to close the application filter configuration window.

5. Click Add to define the Web-Based-File-Sharing application filter:

Name	Type Web-Based-File-Sharing
Subcategory column	Select file-sharing
Technology column	Select browser-based

Click OK to close the application filter configuration window.

6. Click Objects > Application Groups

## 7. Click Add to define the Known-Bad application group

Name : Type Known-Bad

Applications: Click Add and select from the drop down menu each of the following:

- Proxies
- Web-Based-File-Sharing

Click OK to close the application group configuration window.

## Update Security Policies

### 8. Click Policies > Security.

### 9. Click Add to define the Block-Known-Bad security policy:

<b>General tab</b>	
Name	Type Block-Known-Bad
<b>Source tab</b>	
Source Zone	Click Add and select Trust-L3
Source Address	Select Any
<b>Destination tab</b>	
Destination Zone	Click Add and select Untrust -L3
Destination Address	Select Any
<b>Application tab</b>	
Applications	Click Add and select Known-Bad
<b>Service/URL Category tab</b>	
Service	Select any from the pull-down
<b>Actions tab</b>	
Action Setting	Select Deny
Log Setting	Select Log at Session End

Click OK to close the security policy configuration window.

### 10. Add the Allow and Log Outbound Security Policy with the following values

<b>General tab</b>	
Name	Type Allow and Log Outbound
<b>Source tab</b>	
Source Zone	Click Add and select Trust-L3

Source Address	Select Any
Destination tab	
Destination Zone	Click Add and select Untrust-L3
Destination Address	Select Any
Application tab	
Applications	Check the Any box
Service/URL Category tab	
Service	Select any from the pull-down
Actions tab	
Action Setting	Select Allow
Log Setting	Select Log at Session End

Click OK to close the security policy configuration window.

11. Use the Move buttons at the bottom of the page to arrange the policies in a logical order. You can also rearrange the rule by clicking and dragging them into the correct order. Confirm that your security list looks like this (order)

- Block-Known-Bad
- Allow-and-Log-All-Out
- Deny-and-Log-Inbound

Make sure any other policies are disabled

12. Click the Commit link at the top-right of the WEBUI. Click OK again and wait until the commit process completes before continuing.

### Verify Internet Connectivity and Application Blocking

13. Confirm that you can surf the Internet, except for being blocked from web-based file-sharing sites like *avoidr.com*

14. Confirm that you cannot reach file-sharing sites using *avoidr.com*



15. Click the ACC tab to access the Application Command Center. Use the drop-down menu in the application section of the ACC to select different ways of viewing the traffic that you have generated.
16. Click on one of the Applications to get more information. A detailed view appears.
17. Click the x in the box in the upper right hand corner to close the detailed view.